STAFF REPORT

TIVERSA, INC.: WHITE KNIGHT OR HI-TECH PROTECTION RACKET?

PREPARED FOR
CHAIRMAN DARRELL E. ISSA
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
JANUARY 2, 2015

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

Table of Contents

Key Findings

- Rather than the cyber "white knight" Tiversa purports to be, the company often acted unethically and sometimes unlawfully in its use of documents unintentionally exposed on peer-to-peer networks.
- At least one Tiversa employee, under the direction of CEO Robert Boback, provided intentionally false information to the United States government on more than one occasion. Boback later provided false testimony about fabricated documents to the U.S. House of Representatives.
- According to a whistleblower, Tiversa fabricated that an Iranian IP address downloaded and disclosed the blue prints for the President's helicopter, Marine One. Tiversa allegedly did so in order to receive press attention for the company. The Committee found that statements made by Tiversa under oath about this matter could not be substantiated.
- After obtaining information on HIV/AIDS patients at a clinic in Chicago, Tiversa employees called the patients, purportedly in an attempt to get the clinic to hire Tiversa. When the clinic refused to hire Tiversa, the company gave the information to a lawyer that worked with the company who filed a class-action lawsuit that eventually settled for a substantial amount of money.
- Tiversa had information about a breach at the House Ethics Committee exposing information about investigations into Members of Congress. Tiversa did not return this information to the Ethics Committee and instead appears to have sought publicity for the leak.
- Tiversa's co-founder claims the company is in possession of a greater quantity of sensitive and classified information than NSA-leaker Edward Snowden.
- Information provided by Tiversa to the FTC through a shell organization known as the Privacy Institute was only nominally verified but was nonetheless relied on by the FTC for enforcement actions.
- Tiversa obtained non-public, advanced knowledge of FTC enforcement actions from which it attempted to profit.
- According to a whistleblower, Tiversa has knowingly accumulated and is in possession of massive amounts of child pornography and classified government documents.

I. *Introduction*

In the summer of 2013, the Committee learned the Federal Trade Commission would bring an enforcement action against LabMD, a Georgia-based cancer screening company, under the guise of its authority under Section 5 of the FTC Act.[1] Serving as the basis for the enforcement action, the FTC filed an administrative complaint against LabMD after the personal information of approximately 9,000 LabMD patients was exposed on a peer-to-peer network.

Tiversa, a Pittsburgh-based company that sells peer-to-peer monitoring services, provided information on LabMD and nearly 100 other companies to the FTC. This information formed the basis for multiple enforcement actions and dozens of warning letters sent by the FTC. In August 2013, Mike Daugherty, LabMD's CEO, expressed concern to the Committee about both the relationship between the FTC and Tiversa, Inc., and the veracity of the information provided by Tiversa. In April of the following year, the Committee became aware of a former Tiversa employee with allegations of substantial misconduct related to Tiversa's dealings with the federal government.

Committee staff interviewed Tiversa's CEO, Robert Boback, on June 5, 2014. Boback's testimony failed to assuage Committee's concerns and instead raised many more questions about the relationship between Tiversa and various federal government agencies. Two days later, Boback was deposed for a second time in the FTC action against LabMD. There were several major inconsistencies between this testimony and the testimony he provided to the Committee only days earlier.[2]

During the course of this investigation, the Committee conducted ten day-long transcribed interviews and reviewed over 50,000 pages of documents. Documents and testimony obtained by the Committee in the course of its investigation displayed a troubling pattern with respect to Tiversa's business practices. Tiversa routinely provided falsified information to federal government agencies. Instead of acting as the "white knight" the company purports to be, Tiversa often acted unethically and sometimes unlawfully after downloading documents unintentionally exposed on peer-to-peer networks. At least one Tiversa employee, under the direction of Boback, provided intentionally false information to the United States government on more than one occasion. This is a crime. In addition, Boback provided false testimony about fabricated documents to the U.S. House of Representatives.

In many instances, documents that Tiversa produced to the Committee pursuant to a subpoena issued on June 3, 2014 lacked important context without explanation. Such gaps prompted the Committee to ask Tiversa's representatives on several occasions whether the company had produced all documents responsive to the Committee's subpoena as well as search terms proposed by Committee staff. Tiversa did not provide the Committee with assurances or a written statement that all documents had, in fact, been produced. Accordingly, the Committee sought to obtain additional information from third parties. These third parties provided a substantial number of documents to the Committee that Tiversa failed to produce. For example, Tiversa never produced documents showing it had advanced non-public knowledge of FTC

[1] Federal Trade Commission Act, 15 U.S.C. § 45 (2006).

[2] The Committee sent Boback a lengthy letter demanding explanations for the inconsistencies. Many questions posed in that letter remain unanswered.

enforcement actions and took steps to profit from that knowledge. The Committee also found that Tiversa withheld from the FTC a series of documents that are inconsistent with testimony company officials provided under oath. Tiversa's lack of cooperation with this investigation, and the withholding of key documents from the FTC, lead the Committee to believe that Tiversa has not produced all relevant documents responsive to this Committee's subpoena.

According to the testimony of a whistleblower and documents obtained in this investigation, Tiversa appears to have provided intentionally false information to this Committee and numerous other federal departments and agencies. Tiversa has further used and overstated its relationships with Congress and federal agencies to advance its unethical business model. The Committee's findings should give pause to any government entities which have relied or are planning to rely on information provided by Tiversa.

II. *Tiversa's Scheme to Defraud the Congress and Executive Agencies*

Several years ago, Tiversa CEO Robert Boback began perpetrating a scheme in which at least one Tiversa employee manipulated documents legitimately found on the peer-to-peer network to show that the documents had spread throughout the peer-to-peer network. For example, Tiversa downloaded a file that computer A shared on a peer-to-peer network. The file could be copied and the metadata easily manipulated thoroughly widely-accessible computer software programs to make it appear that it had been downloaded by computers B, C, and D, and thus spread throughout the peer-to-peer network. Tiversa relied on the manipulated documents to create a need for their "remediation" services and to grow the company's reputation through press statements and manipulation of media contacts. Boback told media contacts that certain documents, including sensitive government documents, spread throughout the peer-to-peer network when in fact they had not.

According to a whistleblower, Tiversa not only provided the manipulated information to its clients, but in some instances also provided false documents to various entities of the United States government, including the Congress and several agencies. Not only is this unethical, but it is illegal to give false information to the United States government.[3] It is also illegal to obstruct a congressional investigation by providing false information to a congressional committee.[4]

[3] See 18 U.S.C. § 1001, which states in pertinent part:

> [W]hoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully . . . makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry shall be fined under this title, imprisoned not more than 5 years. . . .

[4] See 18 U.S.C. § 1505, which states in pertinent part: 18 U.S.C. § 1505 states, in pertinent part:

> Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States, or the due and proper exercise of the power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress—

Throughout this investigation, the Committee routinely found that information provided by Tiversa either could not be verified, or simply did not make sense. Part of the story always seemed to be missing. The whistleblower's testimony that Tiversa routinely falsified documents, however, filled in these gaps.

III. *Tiversa's Lack of Cooperation with this Investigation*

Over the course of this investigation, Tiversa failed to provide full and complete information to the Committee. On multiple occasions, the company received documents from third parties witnesses responsive to the Committee's subpoena and other document requests, but not produced by Tiversa.

The Committee issued a subpoena to Tiversa on June 3, 2014. The subpoena requested documents responsive to eleven different requests, including:

1. All documents and communications referring or relating to work performed by Tiversa, Inc. on behalf of, in conjunction with, or provided to, any department, agency, or other instrumentality of the U.S. Government.

2. All documents and communications referring or relating to work Tiversa, Inc. performed for the Federal Trade Commission.

* * *

4. All documents and communications referring or relating to internet protocol addresses that Tiversa, Inc. provided to any department or agency of the U.S. Government.

* * *

7. All documents and communications referring or relationg to LabMD, Inc.[5]

Tiversa failed to fully comply with the subpoena. A third-party witness provided numerous documents to the Committee in which Tiversa discussed information it provided to the FTC, and knowledge it had of upcoming FTC enforcement actions, with that third-party. Tiversa failed to produce these documents to the Committee despite their clear responsiveness to the subpoena.

Tiversa withheld additional relevant documents responsive to subpoenas issued by the Committee and the FTC from both entities. In October 2014, Tiversa filed a Notice of

---

Shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both.

[5] H. Comm. on Oversight & Gov't Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014) [hereinafter Tiversa OGR subpoena].

Information in the LabMD FTC proceeding.[6] Tiversa included two e-mails from 2012 as exhibits to the Notice of Information, claiming that the e-mails demonstrate that Wallace could not have fabricated the IP addresses in question. Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission to the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. Tiversa has not explained how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information supporting their position that the documents undermine what they assume to be Wallace's testimony.

Tiversa further failed to fully respond to a subpoena issued by the Federal Trade Commission. As discussed in more detail below, the FTC served Tiversa with a subpoena for documents related to its administration action against LabMD, a Georgia-based medical testing laboratory.[7] Among other categories of documents, the subpoena requested "all documents related to LabMD."[8] In responding to the subpoena, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

Finally, after the Committee learned of Tiversa's involvement with the Open Door Clinic, an AIDS clinic servicing low-income patients outside of Chicago, Tiversa produced selected documents about its involvement with the Open Door Clinic. Committee staff requested specific additional information, including any forensic analysis done by Tiversa of the Open Door Clinic files. Tiversa, through its attorneys, told the Committee that it only analyzed one of the numerous files that it found on the peer-to-peer network about the Open Door Clinic.[9] In fact, as discussed below Tiversa provided extensive forensic services, including two versions of a forensic report, free of charge to Michael Bruzzese. Bruzzese filed a lawsuit against the Open Door Clinic after receiving information from Tiversa. Tiversa never produced the reports to the Committee. Tiversa's withholding of these reports in the face of a direct request from the Committee, and its false claim that it did not analyze most of the Open Door files, is unacceptable.

Given these numerous instances in which Tiversa failed to fully provide information to the Committee and the FTC, the Committee strongly believes that Tiversa may be withholding additional relevant documents. Tiversa's failure to produce numerous relevant documents to this Committee and the FTC, at a minimum, demonstrates a lack of good faith. At worst, Tiversa intentionally withheld documents and other information in the face of multiple subpoenas. Either way, Tiversa's actions call into question the credibility of the company and its CEO, Robert Boback, as a source of information for the FTC.

---

[6] Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014) [hereinafter Notice of Information]. Chief Administrative Law Judge D. Michael Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose." Order on Respondent's Motion to Strike, In the Matter of Lab MD, Inc., No. 9357 (Nov. 19, 2014).

[7] Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC subpoena].

[8] *Id*.

[9] Letter from Reginald J. Brown and Madhu Chugh, Wilmer Hale, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2014).

Boback created a culture of intimidation at Tiversa. The Committee has unfortunately learned that Boback is continuing his intimidation tactics toward former employees that have cooperated with this Committee's investigation. Tiversa has refused to pay legal fees that Gormely accrued while cooperating with this investigation and the FTC matter against LabMD, despite an agreement with Tiversa that he would be indemnified.[10] Boback has further sued Richard Wallace and lawyers representing LabMD in a defamation action in Pennsylvania. The suit against Wallace effectively questions Mr. Wallace's Constitutional right to speak with Congress after the Committee approached him with questions related to allegations about Tiversa. These are clear instances of witness intimidation and interference with a congressional investigation on the part of Boback and Tiversa.

IV. *Tiversa, Inc.*

A. Background on the company

Robert "Bob" Boback and Samuel Hopkins founded and incorporated Tiversa, Inc., a privately-held corporation headquartered in Pittsburgh, Pennsylvania, in January 2004.[11] Prior to joining Tiversa, Boback was a practicing chiropractor who dabbled in other activities including buying and selling residential properties and selling cars on eBay.[12] Hopkins, a high-school dropout, wrote the source code for the proprietary technology that Tiversa later patented.[13] Hopkins sold his shares in Tiversa for approximately $3.5 million and left the company in 2011.[14] Boback is currently the Chief Executive Officer.[15]

Tiversa promotes itself as a company of "cyberintelligence experts."[16] The company maintains an impressive roster of Advisory Board members, including retired General Wesley Clark; Howard Schmidt, the former Cyber-Security Coordinator for President Obama and previously for President Bush; and Maynard Webb, the former CEO of eBay.[17] The Advisory Board met on one occasion in January 2006.[18]

According to Tiversa's website, the company "provides P2P Intelligence services to corporations, government agencies and individuals based on patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day. Requiring no software or

[10] E-mail from Dwight Bostwick, Att'y for Christopher Gormley, to H. Comm. on Oversight & Gov't Reform Majority Staff (Nov. 20, 2014, 4:40 p.m.).
[11] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback (June 5, 2014), at 7 [hereinafter Boback Tr.].
[12] *Id.* at 7.
[13] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Samuel Hopkins (July 29, 2014), at 115, 56 [hereinafter Hopkins Tr.]; Boback Tr. at 56.
[14] *Id.* at 8.
[15] Boback Tr., at 8.
[16] Tiversa, Company Overview, http://www.tiversa.com/about/ (last visited Sept. 15, 2014).
[17] *Id.*
[18] Boback Tr. at 29.

hardware, Tiversa can locate exposed files, provide copies, determine file sources and assist in remediation and risk mitigation."[19]

On July 24, 2007, during the tenure of Chairman Henry Waxman, Boback testified at a hearing before this Committee titled, "Inadvertent File Sharing Over Peer-to-Peer Networks."[20] Boback's 2007 testimony focused on the "privacy and security threats [that] are caused by inadvertent misuse of P2P file sharing software," and his company's work in this area.[21] On July 29, 2009, when Rep. Edolphus Towns served as Committee Chairman, Boback again testified about Tiversa's work in the area of P2P filing sharing and data security breaches.[22] One particular statement garnered a great deal of attention from Members of the Committee and the national media. Boback testified:

> In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.[23]

During this hearing, Boback also provided information on files Tiversa obtained from numerous other companies and non-profit groups, including the Open Door Clinic that Tiversa had "discovered" on the peer-to-peer network.[24]

According to a customer presentation document, Tiversa began working with U.S. government in the spring of 2004. Tiversa claims to have worked "exclusively with the CIA, DoD, DHS, FBI, JCS, and USAF regarding the disclosure of CLASSIFIED [*sic*] information."[25] In reality, Tiversa may not have worked with some of these agencies at all. With others, its relationships were extremely minimal. Overall, the company's claims are overstated.

From 2008 to 2009, Tiversa frequently contacted non-client companies whose documents it discovered on peer-to-peer networks. Under a "duty of care" policy, Tiversa notified companies whose information they found on peer-to-peer networks, and provided them with examples of the exposed documents.[26] Boback explained that by providing this information, Tiversa was essentially providing a public service. In practice, however, Tiversa provided very minimal information to the affected companies. The Committee's investigation found that Tiversa typically provided one document. Even though Tiversa's systems automatically captured other relevant information, such as the IP address from which the

---

[19] *Id*.
[20] Peer-to-peer networks are often referred to as "P2P" networks.
[21] *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight Gov't Reform*, 110th Cong. (2007) (statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.).
[22] *Inadvertent File Sharing Over Peer-to-Peer Networks: How It Endangers Citizens and Jeopardizes National Security*, 111th Cong. (2009) (statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.).
[23] *Id*.
[24] *Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. at 12 (July 29, 2009) (testimony of Robert Boback, CEO of Tiversa, Inc.).
[25] [TIVERSA-OGR-0021275].
[26] Hopkins Tr.,at 205-06.

document was shared, Tiversa would not provide this information to a company unless it purchased Tiversa's services.

During the course of this investigation, the Committee spoke with several companies that chose not to hire Tiversa. In addition, the Committee located one company that did enter into a contract with Tiversa. Tiversa told the company that it spent a great deal of time "investigating" the source of the peer-to-peer leak, at high cost to the company. It appears, however, that Tiversa only provided information its systems automatically downloaded, such as the IP address that leaked the documents.[27] Tiversa further represented to this company that, in order to identify whether any of its computers had peer-to-peer software, it would have to access the company's network remotely and run a search. Tiversa lacks the capability to access a client's network remotely. In this instance, it seems likely that it "identified" the computer using peer-to-peer software by simply looking at the IP address of the computer that shared the confidential document. When the Committee asked Tiversa about its ability to remotely access client computer, Tiversa responded that it never made such a claim to any client.[28]

In his transcribed interview, Samuel Hopkins described Tiversa as "a highly ethical company."[29] After a lengthy investigation, the Committee believes otherwise.

B. Tiversa's claimed abilities to monitor and track files and users on the peer-to-peer network are exaggerated.

Tiversa's business model relies on technology developed by Hopkins, including its trademarked and patented Eagle Vision X1 and Covio. Tiversa claims to have the ability to provide "true cloud security" by seeing the entire peer-to-peer network."[30] Further, Tiversa states that its technologies can "detect and record user-issued P2P searches, access and download files available on the P2P networks, determine the actual disclosure source of documents, track the spread of files across the entire P2P networks [*sic*], and remediate P2P file disclosures."[31]

Tiversa claims that its technology "enables us to view the entire network and thus provide real-time, actionable information regarding sensitive file disclosures related to your organization."[32] In 2007, Boback's written testimony submitted to the House Oversight Committee summarized Tiversa's technological capabilities. Boback wrote:

> Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, **Tiversa can see the P2P network in its entirety in real time.**

[27] Briefing by Company A to H. Comm. on Oversight & Govt' Reform (July 16, 2014).
[28] Letter from Reginald Brown, Att'y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 2, 2014).
[29] Hopkins Tr.at 54.
[30] Tiversa Learning Ctr., *Key Concepts*, http://www.tiversa.com/learningcenter/resources/keyconcepts/.
[31] Marine One forensic report, pg. 2.
[32] Tiversa Learning Ctr., *FAQ/Misconsceptions*, http://www.tiversa.com/learningcenter/resources/faq/.

> With this platform, **Tiversa has processed as many as 1.6 billion P2P searches per day**, more than the number of web searches entered into Google per day.[33]

It is disputed, however, how many files Tiversa downloads daily off the peer-to-peer network. According to Jason Schuck, Tiversa downloads "maybe a million" files daily.[34] However, according to Boback, Tiversa downloads "the equivalent of the Library of Congress every three or four days."[35] The Library of Congress is the largest library in the world, with more than 158 million items, including more than 36 million books and other print materials, 3.5 million recordings, 13.7 million photographs, 5.5 milion maps, 6.7 million pieces of sheet music, and 69 million manuscripts.[36] In essence, Tiversa claims to be able to see the entire peer-to-peer network, instead of a smaller subset as seen by an individual user.

At the time of the leaks discussed in this report, Tiversa used generic and client-specific search terms, such as "reports," "credit card," or "secrets" to query the peer-to-peer network.[37] Even Tiversa analysts could not explain exactly how Eagle Vision keyed into the terms to download them into the data store; that is, analysts did not know definitively whether any document was in the data store due a search term hitting on the file's name, for instance; the search term in the body of the file; or the search term in the name of a folder containing the file. Keith Tagliaferri, Tiversa's Senior Vice President of Operations, and the individual in charge of Tiversa's analytical work, stated:

> I'm not well versed enough on the technology and how it works to know exactly how things key off and what could have downloaded this and that.
>
> I'm aware of all different types of scenarios that can happen as far as why and when we download files. You know, one is matching a key term within a file title. Another is matching a key term within the content of a file.
>
> I've read research that indicates that a folder name can hit on a file. So, for example, if you have a folder called "Work" and somebody searches for "Work," the results that come back are all of the files that are within that folder.
>
> There's also a concept of browse host on peer-to-peer that I'm not sure if our systems have the ability to do or not. But you can literally go to an IP once you find one file and hit "Browse Host" and download all the files from that IP.

---

[33] *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight Gov't Reform*, 110th Cong., at 20 (2007) (written statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.) (emphasis added)

[34] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Jason Schuck, at 12 (Aug. 1, 2014) [hereinafter Schuck Tr.]

[35] Boback Tr. at 143.

[36] Library of Congress, Fascinating Facts, http://www.loc.gov/about/fascinating-facts/ Fascinating Facts (last accessed Dec. 22, 2014).

[37] Hopkins Tr. at 74.

> So there's all kinds of different scenarios that can occur to cause files to be downloaded. I'm not well versed enough on the technical side of our systems to know exactly what would trigger files to be downloaded.[38]

To Tagliaferri's knowledge, there was no way to verify by what search term a document was found and downloaded into the data store.[39]

Tiversa's data store collects and accumulates all the information that is found by Eagle Vision; no documents are deleted.[40] Information enters Tiversa's data store, or repository of databases, in two ways. Either Tiversa's Eagle Vision software downloads the information from the peer-to-peer network, or the information is found independently from Eagle Vision and "injected" into the data store through an application called the Data Store Importer. Schuck described the application in the following way:

> Q. **So analysts have the ability to, I guess, inject files into the data store using the Data Store Importer program?**
>
> A. **Correct**.[41]
>
> * * *
>
> Q. How does it -- if I'm an analyst and I have a file that I want to put into the data store using this program, do you know what steps I take to do that?
>
> A. Sure. If the file is in the correct format, you would place it in a pickup folder.
>
> Q. What does it mean to have a file in the correct format?
>
> A. So depending on the IP address that it was downloaded from, that would be prepended to the original file name.
>
> Q. Who prepends the IP address?
>
> A. Again, you're talking about for the Data Store Importer, right?
>
> Q. Yes.
>
> A. That would be whoever's bringing it in.

[38] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of KeithTagliaferri, at 106-07 (June 17, 2014) [hereinafter Tagliaferri Tr.].
[39] *Id*. at 107.
[40] *Id*. at 88-89.
[41] Schuck Tr. at 19.

Q. Are you aware of specific occasions on which the data store importer was used by analysts to put files into the data store?

A. No, not offhand. That's, again, that's even though I oversee that, I'm not the one that's actually doing that. That would be the analyst.

Q. To your knowledge, has the Data Store Importer been used to put files into the data store?

A. I would assume so, yeah.[42]

Eagle Vision directly downloads documents that either directly hit on a Tiversa search term, or are related to a Tiversa search term (i.e., other documents shared by a user also sharing a document that hits on a search term).[43] According to Hopkins, the creator of the technology, the system does not distinguish between downloaded and injected files.[44] Tiversa, through its attorneys, stated that analysts can "usually" tell if a file is downloaded or injected, but did not explain how its analysts can make that determination.[45] This distinction is critically important, as it would aid in understanding more fully Tiversa's actions.

Tiversa's Covio system indexes the IP address of all files it downloads from the peer-to-peer network. Every time a document containing a search term is shared on the peer-to-peer network, Tiversa's system downloads the document and indexes it according to the IP address from which it was downloaded. Even if the document is exactly the same, the system will automatically re-download it and index it with the new IP address.[46] In this way, Tiversa can determine if a file is spreading, or being shared, throughout the peer-to-peer network.

Boback, however, has offered the Committee conflicting information about whether Tiversa's technology actually does have the capability to automatically download and index documents as they spread throughout the peer-to-peer network. For example, according to Boback, Tiversa never downloaded a copy of a document belonging to LabMD, a cancer screening company, from one of LabMD's computers in Georgia.[47] This document is at the heart of an ongoing FTC action against LabMD. Yet, the document hit on a search term provided by a client, and Tiversa does claim to have downloaded the file from several other IP addresses because of the search term.[48] Tiversa has never been able to explain to this Committee why its systems did not automaticallydownload the file from LabMD but did download the document from so many other IP addresses. Either Tiversa's technology can not do what Boback and Hopkins claim it can do, or Boback provided false information to the FTC and this Committee about Tiversa's downloading of the LabMD document.

---

[42] Schuck Tr. at 20-21.
[43] Hopkins Tr. at 43.
[44] *Id.* at 75.
[45] Letter from Reginald Brown, Att'y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 2, 2014).
[46] Hopkins Tr. at 40.
[47] *Id.*; *see also* Tiversa, Forensic Investigation Report – LABMD0001 (June 4, 2014).
[48] Boback Nov. 2013 FTC Tr. at 41 ("I never downloaded the file from them. They only responded to the hash match.").

Further, Tiversa has not taken steps to screen for illegal content, such as child pornography, before it is downloaded into the data store. In fact, analysts say that it is entirely possible that child pornography is sitting in Tiversa's data store currently. According to a whistleblower, Tiversa has knowingly accumulated and is in possession of massive amounts of child pornography. Tagliaferri stated that he had "heard anecdotally that there may be child pornography" downloaded into the data store.[49] He explained that "as part of that information that's being pulled down, you know, I suppose anything -- anything could come back. You know, it could be Word documents. It could be .pdf's. It could be images. It could be, you know, whatever."[50]

According to Tiversa, The system also "records all user-issued P2P searches," meaning that Tiversa can see a search and record it.[51] Typically, Tiversa can only see the queried search, and cannot identify the user issuing the search. Under very narrow circumstances, Tiversa can determine the IP address of the user issuing a search. Hopkins described Tiversa's limited ability to identify the IP address issuing a search. He stated:

> [The search request] goes to the first three people, they hand it to all the three people there, so it's three and then it's what, nine, so forth. But it only goes five hops. So the three people that I'm connected to, that's the first hop. . . . After five hops, it's dropped off the network. But if you're connected to the three people and the search is one hop away, then you know it came from one of the people you're connected to. But out of the 3,000 people, three people in a security world is nothing.[52]

Thus Tiversa can only determine the IP address of a user issuing the search if Tiversa is one of the three users directly connected to the searcher.

Boback, however, has exaggerated Tiversa's ability to determine the user issuing a search over the years. In 2011, Tiversa claimed to have information that Wikileaks was obtaining information from peer-to-peer networks.[53] Boback claimed that "Wikileaks is doing searches themselves on file-sharing networks."[54] He continued, "It would be highly unlikely that someone else from Sweeden is issuing those same types of searches resulting in that same type of information."[55] Boback further explained that in a one-hour period in February 2009, Tiversa detected four Swedish computers issue 413 searches.[56]

As explained to the Committee by Hopkins, however, Tiversa can only identify the IP address and geographic location of a computer issuing a search if Tiversa is one of only three peer-to-peer users directly connected to that computer. Otherwise, Tiversa can only see the search request, and not the user or location of the user issuing the search. Given the limitations of Tiversa's technology, Boback's statements are very likely exaggerated, if not outright false.

---

[49] Tagliaferri Tr. at 90.
[50] *Id.* at 91.
[51] *Id.* at 160.
[52] *Id.* at 169.
[53] Michael Riley, *Wikileaks May have Exploited Music, Photo Networks to Get Data*, BLOOMBERG (Jan. 20, 2011) http://www.bloomberg.com/news/2011-01-20/wikileaks-may-have-exploited-music-photo-networks-to-get-classified-data.html.
[54] *Id.*
[55] *Id.*
[56] *Id.*

Tiversa also claims that it can "remediate" damage from a document leaked over the peer-to-peer network. Tiversa, however, cannot remove an exposed document from the peer-to-peer network. Instead, Tiversa is limited to sending take-down notices to the internet service provider of the IP address. The success of the take-down notices depends, in part, on the location of the ISP.[57]

C. The Marine One leak

In early 2009, Tiversa's reputation exploded when the company disclosed that it found blueprints for Marine One on a computer in Iran. A whistleblower stated to the Committee, however, that Tiversa only found on the blueprints on a government contractor's computer. Tiversa then manipulated the document by prepinning an Iranian IP address to make it appear that the plans had been downloaded in Iran via the peer-to-peer network. At Tiversa's request, the Committee spoke with multiple federal agencies involved in the investigation into the Marine One leak. The Committee reviewed documents provided by Tiversa, including a forensic report prepared by Tiversa in June 2014, and received briefings and documents from federal agencies involved in the government's investigation of the leak.[58] The Committee found that statements made by Tiversa about the Marine One leak could not be substantiated.

On September 17, 2007, Tiversa "detected" the Marine One file as being shared on the peer-to-peer network. Tiversa's Eagle Vision software did not download this file automatically. Instead, a Tiversa analyst found the file using a stand-alone computer to search the peer-to-peer network. Tiversa determined that a government contractor was sharing the document on a peer-to-peer network.[59] That a contractor inadvertently shared the document on the peer-to-peer network is not in dispute. Tiversa, however, additionally claimed that a computer located in Iran downloaded and shared the file. These explosive allegations garnered large amounts of publicity for the company.

Tiversa claims that on February 25, 2009, it found that an Iranian computer was in possession of the same Marine One blueprints previously shared by the government contractor. According to Tiversa's forensic report, the Iranian computer disclosed the document on the peer-to-peer network between October 27, 2006 and February 25, 2009.[60] Thus, Tiversa conveniently found the document on the network the very last day it was made available by the Iranian computer. The fact that the Iranian computer ceased sharing the document made it next to impossible for any agencies Tiversa alerted after February 25 to determine whether that computer was in fact in possession of the Marine One file.[61]

---

[57] Tagliaferri Tr. at 120, 161.
[58] All information contained in this report was provided to the Committee in an open and unclassified setting.
[59] Forensic Report at 4.
[60] Forensic Report at 10.
[61] If the computer was still sharing the file after Tiversa reported its purported discovery, then individuals investigating the leak could have determined whether the document was, in fact, sharing the file using the peer-to-peer network.

The Committee spoke with Tim Hall, a former NCIS employee who investigated the Marine One leak, on multiple occasions. Hall is now the Director of Government Services at Tiversa.[62] Hall told the Committee that another federal agency verified the information provided by Tiversa about the Marine One leak—specifically, that another agency verified that the file was being shared by a computer with an Iranian IP address. Hall testified:

> Q. And do you know if the information was verified by other task force members?
>
> A. Yes.
>
> Q. How do you know that?
>
> A. Because we worked hand in hand with them daily, just multiple conversations.
>
> Q. Were you ever told how the information was verified?
>
> A. No.
>
> Q. Was all information passed on to other task force members to be verified, to the best of your recollection?
>
> A. Yes. Yes.[63]

Tiversa's counsel also repeatedly told the Committee that the federal government verified the information Tiversa provided about an Iranian computer being in possession of the Marine One document. But that is simply not the case. The Committee learned from NCIS that the joint task force investigating the incident was only able to verify that the IP address provided by Tiversa was located in Iran.[64] The agents did not verify whether that computer actually possessed the Marine One file as this was outside the scope of the investigation.[65]

Given the amount of time that has passed, it is not possible to verify today whether the Marine One file ever spread to a computer in Iran. The Committee has great doubts, however, about Tiversa's story. Tiversa discovering that the document had spread to Iran on the very last day that the Iranian computer allegedly disclosed the file is far too convenient. Further, the Iranian computer purportedly shared the computer for over two years before Tiversa located the file. According to Tiversa, the Iranian computer was in possession of the file in September 2007, when Tiversa initially found that a government contractor improperly shared the document. Yet, Tiversa did not locate the file on the Iranian IP address at that time.

---

[62] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Timothy Hall at 26 (Sept. 3, 2014) [hereinafter Hall Tr.].
[63] Hall Tr. at 25-26.
[64] Briefing by Naval Crim. Investigative Service to H. Comm. on Oversight & Gov't Reform Majority and Minority Staff (Sept. 5, 2014). In the course of the investigation, the Committee received a document from a Tiversa whistleblower listing hundreds of IP addresses in rogue nations around the world.
[65] *Id*.

Tiversa has also not been able to explain to the Committee how it finally learned in February 2009 that the file spread to the Iranian computer. A Tiversa analyst found the original file in 2007, meaning that either no word in the document hit on a Tiversa search term, or Eagle Vision did not download the document when it should have done so.[66] Given that Eagle Vision also did not download the document between September 2007 and February 2009, it would appear that no word in the document hit on a Tiversa search term.[67] So, what prompted Tiversa to search for the document again in late February 2009? That the document does not appear to have been downloaded by Eagle Vision makes the fact that Tiversa downloaded the document on the very last day it was shared by the Iranian computer even more fortuituous.

The story is complicated, to be sure. But Tiversa's complicated tale about this leak unwound when the Committee heard from a whistleblower. According to the whistleblower, Tiversa fabricated that the Iranian IP address downloaded and disclosed the Marine One file. Tiversa allegedly did so in order to receive press attention for the company. This is a very serious allegation—one outside the capabilities of the Committee to verify. If true, then Tiversa provided knowingly false information to numerous agents of the federal government, including this Committee, and wasted federal resources as numerous agencies investigated a fraudulent report. Additionally, the publicity associated with this breach allowed Tiversa to exaggerate the degree to which U.S. intelligence was vulnerable to P2P leaks and sell itself as the solution.

D. Boback created a hostile work environment at Tiversa

Not only does Boback appear to have routinely exaggerated the technological capabilities of Tiversa, but he also created a hostile work environment and retaliated against employees who questioned him. In fact, numerous witnesses put Boback at the center of a hostile work environment at Tiversa. One Tiversa employee stated that he "had significant concerns about [Boback's] ability to execute his job as CEO."[68] The employee brought his concerns to a board member, citing Boback's role in the "creation of a toxic environment," "certain bullying incidences," and "certain practices that I thought were reckless or inappropriate."[69] A faction of employees, led by Boback, frequently left work, offended other employees, and engaged in unprofessional behaviors, including carrying guns to work.

Boback left the office frequently, sometimes for multiple days. In one instance, in early 2008, Boback left with Richard Wallace, the Director of Special Projects at Tiversa, "to pick up

[66] As explained above in Section IV(B), Tiversa's technology should download a document containing a search term each time it spreads throughout the peer-to-peer network. Here, the Iranian computer downloading and sharing the document would create a new document in the eyes of the Eagle Vision system. If the document contained a search term, then it should have been downloaded. If the document contained a search term but was not downloaded for some reason, then Tiversa's software failed to operate as advertised.

[67] Given the magnitude of the discovery, the Committee does not understand why Tiversa would not input key terms from the Marine One document into its automatic download system. Given the gap in time between the discovery of the two documents, either Tiversa neglected to perform this basic task for a leak of great national security significance, or its systems failed to perform as advertised.

[68] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Christopher Gormley, at 27 (July 14, 2014) [hereinafter Gormley Tr.].

[69] *Id.* at 27.

a car in Atlanta."[70] They were scheduled to be gone for only a day, but were instead gone two days.[71] A former Tiversa employee said that this was a frequent habit: "Mr. Boback would generally come in late in the morning and leave fairly early in the afternoon as well... I'm not sure where he was during those hours."[72]

Boback encouraged imappropriate banter and comments by employees that detracted from the professional atmosphere and mission of Tiversa. One former employee testified:

> Q. I'd like to start with a little bit of follow-up from the last hour. You were discussing with my colleagues some joking emails, I guess, for lack of a better term, that Mr. Wallace sent, and I believe you described that there were many of these emails that were sent among a certain group of people. Is that accurate?
>
> A. I wouldn't say so much many emails, but there was a lot of banter, I guess, orally. And I'd say there was a certain amount of that you'd expect, but some of it in this case was out of line for what I considered a company of what we were trying to create was.
>
> Q. Was Mr. Boback ever involved in this banter?
>
> A. Yes.
>
> Q. Did he ever express that he felt the banter was not appropriate for the workplace?
>
> A. No.
>
> Q. Did he make joking comments along the same lines of what other employees were saying?
>
> A. Yes.[73]

Boback routinely made offensive remarks to Tiversa employees, creating an atmosphere of harassment and intimidation. One employee described described Boback's inappropriate comments to the Committee:

> A lot of, I guess, homosexual jokes, right? This or that. I mean, something akin to being in a junior high school playground, and it was fairly rampant, and it was just, you know, difficult to not engage in that… one particular story that I do remember is we had a company meeting. Well, I entered the company meeting, and one of the -- and I don't remember who -- made a remark to that effect, and everyone in the meeting laughed,

[70] *Id.* at 38.
[71] *Id.* at 38.
[72] *Id.* at 40.
[73] *Id.* at 79.

> including Mr. Boback. It was clearly uncomfortable for many in the room. And I think, you know, those are the issues I was trying to convey to the board member, just that we can't have an environment like that in today's day and age, and that can we at least put some boundaries to that kind of behavior inside the office.[74]

Gormley described another instance of Boback acting in an unprofessional manner :

> I remembered receiving an email that copied a colleague of mine, Griffin Schultz, that said, you know, "Chris, you should get a job as a Presidential piss boy," which just out of, you know -- stated very clearly it was a joke, but he stated it, that I should get that kind of job.[75]

* * *

> Q. What did you understand him to mean by that phrase?
>
> A. I don't know what was in Mr. Boback's mind when he made that, other than the email said what it said. The context was Mr. Schultz was trying to make an introduction to some congressional staffers or somebody that he had known in the past, and there may have been some mention of various roles, but not Presidential piss boy, but it may have been in the context of that. And then he said, Chris, that's a great job for you, Presidential piss boy, and Griffin Schultz was on that email as well me.
>
> Q. Do you recall when that email was sent?
>
> A. That would have been, I believe, April 2008. It was in 2008. I don't -- I think it's April.[76]

Boback also referred to "teabagging" with Wallace and Hopkins while at work. One employee described conversations he overheard at the office:

> I would be at my desk listening to them talk about playing Halo 3 and how they teabagged this person from Russia or this person from -- but it was extremely rampant to the point where it was very disruptive to the business. So that was one of the things I reported to the board member, to say we need to get them engaged back in the business, because, you know, they were needed for doing business, and I, again, didn't think that was an appropriate conversation for a work office.[77]

---

[74] *Id.* at 79-80.
[75] *Id.* at 19-21.
[76] *Id. at* 57-58.
[77] *Id.* at 179-80.

Boback also condoned employees carrying and wielding firearms , and brought a gun himself to the office on multiple occasions. Transcribed interviews with Tiversa employees reflect that both Sam Hopkins, the co-founder of Tiversa, and Boback carried guns while at work at Tiversa. Sam Hopkins was aware that Boback carried a gun around at the office:

> Q. Did you ever see any other weapons in the office of any kind?
>
> A. Bob had a handgun that I saw a few times.
>
> Q. And did he show you the gun when he was in the office?
>
> A. In his office, yeah.
>
> Q. Why did he -- do you know why he showed you this gun or do you–
>
> A. You know, just two guys talking and he had known that I was carrying.[78]

Keith Tagliaferri saw Boback "walk by with [a gun case]," although he did not look inside the case.[79] Christopher Gormley was also aware that Boback carried a gun at work. Boback even showed Gormley his gun:

> Q. And what was the context of the meeting at which Mr. Boback pulled out his revolver and showed it to you?
>
> A. He just came in. He'd come in a lot. I mean, his office was close to mine. And, I believe, that day -- and I can't be certain of this, but I'm pretty sure that he had taken a number of individuals from the company out to shop for guns at a gun store.
>
> Some people from the company actually departed for the afternoon, and I didn't know where they went. Which was a fairly common activity, that he would disappear for long periods of time. But this particular afternoon, I mean, that was my belief at the time, that they went to a gun store, and this may have been a purchase then. But it was showing me that he had purchased this or had this. I wasn't sure whether he actually got it at the gun store or not. But that activity occurred that day.
>
> Q. Do you recall approximately when this took place?
>
> A. Yes. Well, let me think. It would've been in the first quarter of 2008, maybe April.[80]

[78] Hopkins Tr. at 150.
[79] Tagliaferri Tr. at 161-62.
[80] Gormley Tr. at21-22.

Gormley also described Boback displaying his gun in an intimidating manner:

> [] I would later discover that, I mean, **Mr. Boback, at least as far as my personal experience went, had certain bullying tendencies**….
>
> On one occasion, he entered my office and, you know, sat at a desk in front of me and reached into his sock holster and pulled out a revolver and showed me its features and functions. And I thought that that was extremely surprising, that somebody would actually have a concealed weapon in the office and then pull it out to me. And I didn't feel like he was going to use it on me, but I thought, what are you doing with this and why are you showing it to me? And I thought that was -- that was one incident. That was pretty stark.[81]

Boback never revealed to the Committee that he brought a gun to work. He was quick to suggest, however, that Hopkins carried a gun to work, out of fear of Wallace:

> [Hopkins] told me years ago, that he purchased a gun and a carry permit as protection against Mr. Wallace solely to protect -- as he felt scared for his physical existence against Mr. Wallace….[82]

Gormley also had personal knowledge of Hopkins bringing a gun to work, including one incident when Hopkins pointed a gun at Gormley:

> Q. You mentioned other Tiversa employees carried weapons in the office. Do you recall which employees did that?
>
> A. Well, one incident I remember **Sam Hopkins had gone and pulled it out and pointed at me down a hallway**.
>
> * * *
>
> Q. Did you feel threatened when Mr. Hopkins pointed the gun at you down the hallway?
>
> A. I didn't feel threatened at the time.
>
> Q. Did Mr. Hopkins say anything when he pointed the weapon?
>
> A. I don't remember him saying anything. It may have been the same day that Mr. -- they all went to the gun store, and I don't know if it occurred after or before Mr. Boback, so I may have been more sensitized to the fact that there were weapons in the office that day, silly as that sounds.[83]

[81] *Id.* at 18-19 (emphasis added).
[82] Boback Tr. at 205
[83] Gormley Tr. at 76 (emphasis added).

Boback also brought swords to the office, and distributed swords to Tiversa employees. According to Schultz, "Bob would hand out a sword to each new employee that he thought represented their character… I believe mine was like a Marine sword or something based on my time at Wharton and a few other things that he thought fit my character… Someone else got the sword Gandalf carried in *The Lord of the Rings* because he thought it fit their [*sic*] personality."[84]

The Committee learned of one instance where an employee attempted to take action against Boback and his intimidation tactics. Gormley described a professional disagreement he had with Boback over handling a forensic analysis issue. In a response that the Committee has found to be typical, Boback sent Gormley a threatening e-mail. Gormley testified about the incident:

> Mr. Boback and I had a dispute as to how to handle the scope of that particular exercise [regarding how narrow or broad search terms should be kept for a prospective client]. I don't think either one of us were right or wrong… I contended that we should provide the whole. He contended that we keep it more narrow.
>
> We had a very stark disagreement on how to handle that…And this was a highly negative—well, a very stark email to this effect sent to me, as well as a phone call later that evening when I was at an event with my daughters at school. And he told me to keep it within the scope he told to me, to keep it, **or else there would be consequences—in other words, either terminations or significant consequences**.
>
> [T]hat's what motivated me to go to Mr. Becker.
>
> **I was actually quite concerned to go to Mr. Becker because I feared retaliation**.[85]

From that point forward, Gormley chose not to confront Boback because he felt that it "usually wasn't very productive, because [Boback] would come at you and tuck it away as something that potentially could be used later."[86]

When Boback heard that a Tiversa employee had approached the board with concerns about his professionalism and leadership, he became irate and sought retaliation:

> I was very concerned about retaliation or being—it turned out that the feedback I gave to Mr. Becker, I believe, was incorporated through various actions the board had taken… [T]here was a point in 2008, in September, early September, where Mr. Boback called me up and said he'd just received a review and some feedback from the board, and one of the elements was that an… employee in the company had given that [negative] feedback. And he was extremely angry about that and **wanted**

[84] Schultz Tr. at 112-13.
[85] Gormley Tr. at 25-26 (emphasis added).
[86] *Id.* at 30.

> **to know who that person was, and he was going to take whatever measures it took to find that out**.
>
> In the subsequent week and a half, **he held individual meetings with each person and also held a group meeting where he asked each person in the executive team, did you say it, did you say it?** And he suspected that [redacted name], an employee of the company, may have been the person. My guess is he also suspected me. I denied that at the time, out of concern for my own wellbeing I guess. But he wouldn't let it go.
>
> * * *
>
> He came into my office, everyone had left, shut the door, sat in the same seat that, you know, the pistol and everything had been pulled out, and basically kept asking me questions in different ways to see if it was me[.]
>
> * * *
>
> Now, he also said that… **he thought it was [redacted] and that I needed to fire [redacted] because he suspected that it was her**. [Redacted] happens to be a personal friend of mine, somebody I brought into the company. So I was in a very conflicted situation, because I either fire somebody that I know didn't do it or I admit that I did it. So I told Mr. Boback that it was me that evening and told him why, you know, went through some of the major reasons that I mentioned that I gave to Mr. Becker.
>
> * * *
>
> But, after that point, **there was a lot of fallout that I believe occurred because of that incident**. And it was a very difficult period for me personally at the time, **because at that point I was ostracized from the rest of the company**, had to apologize to different people within the company for having went [*sic*] out the chain of command and saying things, that, in Mr. Boback's view, weren't true.[87]

Soon after, in September 2008, Gormley was demoted from COO to "Vice President of Data."[88] Boback explicitly told Gormley that the demotion was the "outcome [of] those discussions with the board."[89] Nonetheless, Gormley tried to perform his new job. Boback, however, refused to let Gormley succeed. Gormley testified::

> This is in 2009, and as part of the data business, I was involved on a potential acquisition of the company by Experian. Mr. Boback and I got into an argument about how to interact with Experian in that discussion. I

[87] *Id.* at 31-32 (emphasis added).
[88] *Id.* at 33.
[89] *Id*. at 33-34.

> wanted Lisa Frankovitch to be the person who would interact with Experian and then have Mr. Boback back her up in the discussions. He didn't agree.
>
> We had a disagreement about that, and **subsequently he just said, "Joel wants you off the deal**," meaning this board member wants me off the deal. This is subsequent to [the]… first board meeting, and I didn't believe that that was the case. I reached out to Lisa Frankovitch, who had that relationship, but then she suggested I talk to Joel directly. I called him up, and he indicated that **he never said that, and he said that I should go talk to Bob and make that clear**. So it was—at the time it clearly caught up with him, no, he didn't, Joel didn't actually state that. So that was one indication.[90]

Gormley was terminated in late 2009, he believesin retaliation for reporting Boback to Tiversa's Board of Directors.[91]

> Boback's intimating comments did not end even after Gormley was fired:
>
> Q. Have you had any other communication with Mr. Boback since your termination? I don't know if threats of litigation counts, but have you had any communication with Mr. Boback following your termination?
>
> A. Yes. The points of communication after termination, I guess the first time he communicated with me, I decided not to sell some options that I owned in approximately 2011, and he sent me an email that started with "LOL, LOL, LOL." That means -- you guys know what that means -- "laugh out loud, laugh out loud." And **he ridiculed me for not selling my options and then made fun of my role as the director of downstream marketing and just sent that to me out of the blue**. And I still have that email. That was 2011.[92]

The Committee has further learned that Boback is continuing his intimidation tactics toward former employees that have cooperated with this Committee's investigation. Tiversa has refused to pay legal fees that Gormely accrued while cooperating with this investigation and the FTC matter against LabMD, despite an agreement with Tiversa that he would be indemnified.[93] Boback has further sued Richard Wallace and lawyers representing LabMD in a defamation action in Pennsylvania. Such witness intimidation tactics are unacceptable.

---

[90] *Id.* at 89-90 (emphasis added).
[91] *Id.* at 87-88.
[92] Gormley Tr. at 147 (emphasis added).
[93] E-mail from Dwight Bostwick, Att'y for Christopher Gormley, to H. Comm. on Oversight & Gov't Reform Majority Staff (Nov. 20, 2014, 4:40 p.m.).

E. Boback has not been forthcoming regarding the nature of his close relationship with Wallace, or the central role Wallace played at Tiversa

In advancing the narrative that Wallace is the source of all of Tiversa's problems, Boback has repeatedly contradicted his own statements to the Committee. Often, instead of answering the question asked, he instead spoke tangentially about Wallace's bad character and dangerous propensities.

Tiversa recruited Wallace in mid-2007.[94] Wallace was given substantial responsibilities at Tiversa. In his professional duties, Wallace was tasked with "reflect[ing] the technology of Tiversa to customers when they would come in."[95] Wallace was "many times called out to be the expert technical person in the data store area of our office."[96] Wallace also was Tiversa's face for the FBI, and spent around 20-30% of his time "doing work related to the FBI arrangement."[97] A former Tiversa employee said that Boback "absolutely" trusted Wallace's work.[98]

Boback would like the Committee to believe that Wallace was and continues to be the source of all of Tiversa's problems. If that were true, Boback would be in gross dereliction of his official duties as CEO of Tiversa. However, accounts of multiple Tiversa employees indicate that Boback and Wallace shared an exceedingly close relationship, and that Boback leveraged his status as CEO to manipulate Wallace to act on his behalf.

Numerous Tiversa employees have characterized Boback and Wallace as close, and testified that the two spent a great deal of time together. As one employee stated :

> **[T]hey were together constantly**… Mr. Wallace tended to know where Mr. Boback was. If you needed to know where Mr. Boback was, you'd ask Rick, or Molly Trunzo would ask Rick, because many times he knew where Bob was.
>
> * * *
>
> **I mean, my perception of Mr. Wallace was that he was Mr. Boback's spy.** And I think one on one I had a decedent relationship with Mr. Wallace, but I think when he was in a group or he was with Mr. Boback, he became different, and he tried to show his worth, I think, in multiple ways with Mr. Boback.[99]

Troublingly, numerous Tiversa employees described Boback and Wallace following cars together. Czarnecki stated that he heard "some kind of talk about [Boback or Wallace using a

[94] Gormley Tr. at 176-77.
[95] *Id.* at 50.
[96] *Id.* at 50.
[97] *Id.* at 86.
[98] *Id.* at 178.
[99] *Id.* at 48-49 (emphasis added).

GPS device] at the old offices"[100] to track a specific individual.[101] Another former employee also heard Boback and Wallace talk about putting a tracking device on a vehicle.[102] Gormley believed that he would be followed after he approached a board member with concerns about Boback's professionalism, "because there was a history of Mr. Boback and Mr. Wallace following people for fun, you know. And so, in this instance, I felt like they may follow me and, you know, a retaliation may occur[.]"[103]

Ultimately, statements made by Boback impugning Richard Wallace simply do not add up with the facts of Wallace's employment while he was at Tiversa.

a. Wallace received only a glowing performance review while a Tiversa employee.

Wallace received one review during his tenure at Tiversa. This review, given in 2008, described Wallace as a talented analyst and consummate professional. Among his "key accomplishments," the review stated that Wallace:

> Led the work and served as an official informant to F.B.I. related to child pornography on P2P file sharing networks. Rick also managed the day-to-day relationships with two F.B.I agents. This work was new to Tiversa and Rick handled the many ambiguities associated with this work in a highly professional manner that was respected by his F.B.I. counterparts.[104]

The review describes Wallace as "critical in aligning Tiversa for a potential deal with the Air Force Office of Special Investigation," and "*instrumental* in a number of press events serving as an expert for reporter research."[105] The review stated that as a cyber forensic analyst, Wallace "monitor[ed] accounts of Cigna, American Express, and PGP and [was] a core Cyber Forensic Analyst with, for example, University of Florida, Wagner, Wachovia, GE." Wallace also "contributed insight into the design and operation of Tiversa F.A.S.T. productivity suite which whwen fully implemented should substantially improve CFA productivity."

The review listed Wallace's strengths as the following:

> Work Ethic
> Rick has an outstanding work ethic and can always be relied upon to put in the extra effort surrounding a project or finding files to support a Tiversa business opportunity. There have been many weekends and/or late nights where Rick has worked extra hours either in the office or at home to make Tiversa's business objectives happen.

[100] H. Committee on Oversight & Gov't Reform, Transcribed Interview of Orion Czarnecki, at 72 (Sept. 16, 2014) [hereinafter Czarnecki Tr.].
[101] *Id.* at 72.
[102] *Id.* at 40-41.
[103] Gormley Tr. at 26.
[104] Tiversa, 2008 Review of Richard Wallace (Aug. 4, 2008).
[105] *Id.* at 1 (emphasis in original).

> Client and Media Relations
> Rick has received exemplary feedback for his work from client contacts most notably from F.B.I. and Cigna. Rick has also managed relationships and provided P2P background to outside parties and media during their investigations of P2P risks.
>
> Drive for new business / press
> Rick is constantly scanning the P2P (literally) for files or individuals that will yield new Tiversa business, yield more tickets for existing Tiversa clients thus strengthening Tiversa's value with existing clients, and finding situations that put the P2P or Tiversa in a strong public relations position. Rick always seems to be able to find a hard hitting file or P2P situation to accelerate our client acquisition, existing relationships or to help serve as a nugget for a powerful news story. For example, recently Rick found a number of American Express internal files in the Philippians [*sic*] which have strengthened our relationship with Amex's CIO and put us in contact with Accenture.
>
> Enthusiasm for the P2P Space
> There is no other person at Tiversa that lives and breathes P2P more than Rick. His level of enthusiasm for finding P2p sourced information is contagious and extremely valuable to Tiversa.[106]

Going forward, the review pointed to two areas in which Wallace could improve. First, the review suggested that Wallace "[c]onsider [d]ownstream [a]ffects [*sic*]" by

> [N]ot only continu[ing] his outstanding work as an individual contributor, but [] seek[ing] to make the whole team more effective, more highly scalable, less Dilbert-like by balancing the short term needs for sales and files with the long term need to make everyone effective and ready to handle more scale. I would ask Rick to please provide me direct feedback on areas that he thinks can be more effective and to **take a leadership role** in addressing the issue.[107]

Second, the review suggested that Wallace pursue searching other peer-to-peer networks for "'veins' of file gold":[108]

> **Rick is a maestro of LimeWire operation and sleuthing. The business benefits greatly every time we find more "veins" of file gold not only including sources on LimeWire, but on wholly new P2P networks.** For instance, the addition of eDonkey to our roadmap was guided by the large magnitude of sensitive files that appeared by using the eMule client in

[106] *Id.* at 1-2.
[107] *Id.* at 2.
[108] *Id.*

> Tiversa's lab. In between leveraging LimeWire for the benefits already highlighted above, I would like Rick to experiment with other clients to discover new caches of files and help guide our product roadmap.[109]

In consideration of his performance, the review noted that Wallace was to be given a 9.8% raise, in addition to the 20.6% Wallace received at the end of 2007. [110] The review concluded by congratulating Wallace on his achievements.[111]

It is not clear who at Tiversa wrote Wallace's review. Gormley stated that he, Schultz, and Boback would have all had input on the review.[112] Although Schultz was Wallace's direct supervisor, and although Schultz reported to Gormley, Boback gave Wallace a direct raise without telling either of Wallace's supervisors.[113] This caused Gormley to think that he, Schultz, and Boback "had split responsibilities for Mr. Wallace."[114]

Tiversa employees characterized their relationships with Wallace as typical professional relationship. Tagliaferri stated that he and other Tiversa employees socialized with Wallace:

> Q. Did you socialize outside of the office with Mr. Wallace?
>
> A. Sometimes. If he would have a bonfire or a Christmas party or something like that at his house then I would attend something like that.
>
> Q. And were these events attended by Tiversa employees generally?
>
> A. Sometimes. There might be, you know, a couple of other Tiversa employees there, and other professionals in the security industry that we all work with that may attend one of his get togethers.[115]

When asked to describe Wallace's professional contribution to Tiversa, Tagliaferri stated:

> [Wallace] found a lot of information that was very sensitive, confidential and bad stuff out on these networks that shouldn't be out there, and he was really good at finding information out on the networks.
>
> And, to that extent, you know, would we have found that information without Rick? I don't know. Maybe we would have**. But the things that Rick found certainly contributed to the company. He was an asset to the company to that extent**.[116]

---

[109] *Id.*at 2-3.
[110] *Id.* at 3.
[111] *Id.*
[112] Gormley Tr. at 205.
[113] Gormley Tr. at 55.
[114] Gormley Tr. at 55.
[115] Tagliaferri Tr. at 156.
[116] Tagliaferri Tr. at 98 (emphasis added).

Boback and Wallace's relationship extended beyond the professional. When Boback and Wallace interacted in the office, it was not through the traditional hierarchical channels:

> Q. Mr. Boback was the CEO, correct?
>
> A. Yes.
>
> Q. And Mr. Wallace was an analyst, correct?
>
> A. Mr. Wallace was an information forensic engineer.
>
> Q. And so, in the corporate hierarchy, Mr. Boback was certainly above Mr. Wallace, correct?
>
> A. Yes, substantially.
>
> Q. Is the type of direction that Mr. Wallace took from Mr. Boback typical to the type of direction that other employees in Tiversa took from Mr. Boback? Or was there something different about the nature of the direction that Mr. Wallace was taking from Mr. Boback?
>
> A. It was much more one-on-one, less hierarchy involved. It wasn't like Mr. Boback went to me and then I went to Mr. Schultz and then Mr. Schultz went to Mr. Wallace to ask him to do something. **It was, "Hey, Rick, you're coming with me," and off he went. Or, "We don't know where Rick is. He's with Bob."** It was much more direct. **So it was independent of any kind of hierarchy that existed**.[117]

Another Tiversa employee verified that even though Wallace was a forensic security analyst, he reported directly to Boback.[118] According to a former Tiversa employee, Boback and Wallace were very close, with Boback exerting greater influence over the relationship:

> Q. Would you describe them as close friends?
>
> A. Yeah, absolutely… **[T]here was nobody that was closer to Bob in the time frame that Rick was there than him**, with maybe the small exception of Mr. Hopkins, but even Mr. Hopkins had his own life, and he just wanted to go do his thing. Mr. Wallace and Mr. Boback were tied at the hip.

[117] Gormley Tr. at 214-15 (emphasis added).
[118] Tagliaferri Tr. at 75 ("[M]y understanding was that he reported to Mr. Boback.")

Q. You would say they're close friends?

A. Yeah, I would say that.

Q. **Would you describe one of them as having a dominant role in the friendship?**

A. **Yeah, Mr. Boback.**

Q. Could I ask why you would say that?

A. Well, Mr. Boback had a bigger house, he had all the little—you know, the toys and games, and so that would certainly lead the way, and just the way they interacted with one another. **It was clear that Mr. Wallace was taking direction from Mr. Boback, not the other way around**.[119]

Boback, on the other hand, has consistently mischaracterized Wallace and his responsibilities to the Committee. When asked a simple question about what duties Wallace performed at Tiversa, Boback could not give a straight answer:

Q. Okay. When Mr. Wallace was employed at Tiversa, which section or sections did he work in?

A. I don't know that he necessary -- he really didn't work in -- he was never a cleared individual, so he never had the clearance portion of it when everyone else went through there**. Mr. Wallace's role at Tiversa was regarding, or most of his work was child pornography**, searching for child pornography and providing it as a confidential informant to the FBI, and also identifying new cyber risks for, you know, educational purposes that he would then provide to me and then whenever I would go, I've traveled around the country training law enforcement for FBI LEEDA, L-E-E-D-A and he would sometimes travel with me and, you know, highlight different risks for the cyber world that law enforcement wouldn't see otherwise.[120]

* * *

Q. Was Mr. Wallace first hired as an analyst?

A. Yes, he was.

[119] Gormley Tr. at 180 (emphasis added).
[120] Boback 62-63 (emphasis added).

Q. And when was he first hired by Tiversa as an analyst?

A. I'm not sure exactly, but I think in 2007, maybe. I'm not sure of the exact date, but the summer roughly, I think I remember around the summer of 2007.

Q. Was Mr. Wallace first hired for his skills as an analyst or for his work with the FBI?

A. No, Mr. Wallace was hired as an analyst. Mr. Wallace was a stay-at-home dad in Illinois and his wife was in the military, and Mr. Wallace ran a Web site called SeeWhatYouShare.Com. Essentially, See What You Share, what he did was, he would search for files leaked or exposed on file-sharing networks and he would publish them on his Web site. Essentially, he was the first iteration of WikiLeaks, but he did it under the SeeWhatYouShare.com website.

So an individual, Tom Sydnor, Thomas Sydnor who used to work at -- work with Senator Hatch in the Senate Judiciary, Tom Sydnor told me about this Richard Wallace and said, hey, you should talk to this guy because he's, you know, in the space that you're in where no one knows anything, he's doing some searches that may be of interest to you, and he said, he's a little different but you should talk to him.

So we flew him to Pittsburgh, we met with him and then we offered him as a job as an analyst and that's how he started, as an analyst in our corporate business and that's what he started with a reporting structure of he reported to an individual by the name of Griffin Schultz who reported to the chief operating officer, Chris Gormley, who then reported to me.[121]

* * *

Q. At what point did Mr. Wallace's work transition from part time for the FBI and full time for the FBI?

A. **Mr. Wallace was very erratic in his time, so I'm not sure. Sometimes you'd see him; sometimes you wouldn't, in the office.** And he was -- I'm not sure. **It was mostly FBI work. Again, he didn't generate revenue so therefore it was hard for me to say**, I couldn't tie it to revenue coming in so I didn't know, you know, what he was doing.

[121] Boback Tr. at 64-65 (emphasis added).

> So he, you know, that's how that went. So, I mean, he was still working as an analyst, obviously, in 2008 and then he, like I said, he was doing both work and then it kind of transitioned out, probably closer to 2009, 2010.[122]

Expanding on the assertion that Wallace did not generate revenue, Boback told the Committee that Wallace and personally received cash payments from the FBI as a confidential informant, while Tiversa did not receive any money as a result of Wallace's FBI affiliation:

> Q. So Mr. Wallace worked with the FBI. It sounds like he was, at times, working in the business-to-government section. Is that fair?
>
> A. But we didn't have any contract with the FBI, so that's why I don't necessarily know where to put him. **He was not a revenue generating** [*sic*]. In fact, recently it's come to light that Mr. Wallace, it's our understanding that **Mr. Wallace was receiving revenue from the FBI as a confidential informant, yet none of that money ever made it to Tiversa**. So he was keeping that money, that cash that was being given to him, at a reported, as we were told a reported $1,000 per child pornography case that he gave to the FBI.[123]

However, a former Tiversa employee told the Committee that Tiversa—or at least Boback—was compensated in cash for Mr. Wallace's work with the FBI:

> Q. And do you know whether Tiversa received any compensation from the FBI for Mr. Wallace's work?
>
> A. Yeah. **They were paid cash. I don't know how much. I recall one instance where there was a bag of cash on Molly Trunzo's desk, and it was apparently from the FBI.**
>
> Q. As someone who was responsible, in part, for –
>
> A. About this much. [Estimating the size of the bag].
>
> Q. -- overseeing financial controls at Tiversa, were you concerned that the FBI was paying the company in bags of cash?
>
> A. Yeah.
>
> Q. Did you raise those concerns with anyone at the company?

[122] *Id.* at 75 (emphasis added).
[123] *Id.* at 63 (emphasis added).

A. This was after my review of Mr. Becker. Yeah, I -- well, I'm trying to remember if I raised those concerns. I definitely raised the concerns during the arbitration hearing, you know, because I wasn't sure whether that was being recorded properly.

The relationship with the FBI itself and how it was set up, I remember Griffin Schultz making a comment and me making a comment at the time as to how we thought it should be handled. And that was another instance of Mr. Boback lashing out at Mr. Schultz. I remember that.

And that was on my -- actually, it was on my comments to Mr. Becker. I remember telling Mr. Becker about any cash and the FBI because I don't know that they were paying us at that time. I think it was just an initial, kind of, trial.[124]

Gormley, the CFO, was apparently not made aware of the cash payments prior to seeing them on Trunzo's desk, and could not say if the money was properly placed in an account.

Later in his transcribed interview, Boback contradicted himself in admitting that Tiversa had received a cash payment from the FBI, although he insisted the money went to Wallace:

Q. But you don't have any specific information about anything that he downloaded?

A. He's a confidential informant, and we didn't know. But as I mentioned before, early on Mr. Frankhouser talked to me about knowing that Rick Wallace was on Tiversa's payroll and downloading child pornography presumably for their prosecutions. He discussed paying Tiversa as a confidential informant, of which I think he did. I mean, he may have -- they may have paid us as a confidential informant a little bit. I could double check. I'm not positive. **They may have paid us some money as a confidential informant**.

Q. So as you understand it, Tiversa is a confidential informant as opposed to Mr. Wallace, personally?

A. I don't know how the FBI designates it, you would have to look. I know that it ultimately became Mr. Wallace. He said to me, he being Mr. Wallace, said to me, along the way that for work he has been doing with the FBI, he was owed some money, and he was owed so much as a confidential informant. It was like $1,000, or $2,000, or something like that.

[124] Gormley Tr. at 209-210 (emphasis added).

> **And he said to me, would I mind if he took that as a bonus because he has been doing so much hard work for this. I said, no, I don't mind, meaning put the cash into the account at Tiversa as we always do, record it, because we wanted our revenue to come up, and then we will add the amount to your check with the proper withholdings**, and that was the last time, thinking back, that was the last time I ever heard anything talked about money paid as any informant and it's my allegation that he continued to take that money, at a rate of roughly $1,000 per case, in cash and he took it. So I reported that to the authorities.
>
> Q. I see. And the FBI was paying Tiversa for the information that Mr. Wallace was providing, is that right; there was some kind of contract?
>
> A. No.
>
> [Att'y] No, he didn't say that.
>
> Q. Nothing?
>
> A. Nothing.
>
> Q. I'm sorry if I misunderstood.
>
> A. Yeah, no. It is my allegation that **Mr. Wallace was paid by the FBI as a confidential informant, from monies that should have been directed through Tiversa because he was doing that under our direction and we were paying him a salary to do that**, as I mentioned to you and he decided to take that money himself, which is larceny. [125]

In a separate instance, Boback described Wallace's professional behavior as "normal" before launching into a tangent about how Wallace had a "revenge-based mentality":

> Q. How often during the course of his employment at Tiversa, if you could describe it for us, was Mr. Wallace in the office? Was it daily?
>
> A. Yeah. I mean, **he was in there like a normal employee, for the most part. I mean, he would come in and leave just normal**.
>
> Q. Earlier today you mentioned he worked from home a lot and you didn't really know what he was doing.

[125] Boback Tr. at 120-122 (emphasis added).

A. Well, he worked -- as I testified to, he told us that the best time to catch child pornographers was in the evening. So his working from home was over the night, like at nighttime.

Q. Okay. So –

[Discussion off the record.]

[Att'y] If you could just be clear on that.

A. So he would be in the office and then he would go home and search. I think that Mr. Wallace searched peer-to-peer quite a bit as a part of his normal -- it was almost like his ritual, if you will, for his life, to where he was always searching.

Like he was always in front of a computer screen and always searching something, either online or searching peer-to-peer, whether it was at the office or whether it was at home. He was always –

Q. Did you find that troubling?

A. I work in tech. Everyone's a little bit different. So, I mean, we have -- in tech, you know, you have different personalities. He was no exception of a different personality.

The downside of one of the things that **you recognize is he had a very revenge-based mentality[.]**[126]

However, Boback described Wallace's duties as much more expansive when the discussion turned to verifying the truth of his testimony before Congress. Boback testified that Wallace was solely responsible for Boback's testimony before this Committee in 2009. Thus, according to Boback, any blame for inaccuracies in the testimony should fall on Wallace. Boback testified:

Q. Did Tiversa employees identify the source of this information other than France? In other words, France got it from somewhere, so do you know where France got it from? Did Tiversa employees determine that?

A. **You're asking me to testify to what someone else did? I have no idea. I was provided information that I testified to, which I believed to be rue and correct, as I just testified to again.**

[126] *Id. at* 202-03 (emphasis added).

Q. Yeah, no, no, I hear you. I'm just asking you if you know anything else about the facts underlying.

A. **I know that Mr. Wallace would have been doing this type of work and provided this information to me, which I then provided, believing it to be true and correct, to Congress.**

Q. Can you tell us with a little bit more specificity what the information Mr. Wallace provided to you was?

A. Sure. Again, this was 5 years ago, but **Mr. Wallace would have been responsible for discussing breached files; finding, downloading breached files; locating the location of where those files came from; and then, you know, articulating that to us**. So, you know, producing that information, so therefore any information that I received regarding where a file came from, who was the disclosing source, the file itself all came from him.

Q. And did he tell you those things?

A. Yes.

Q. The source?

A. Yes.

Q. The location, the specific location?

A. Yes.[127]

* * *

Q. Just to clarify for us, my understanding -- and please correct me if I'm wrong, but my understanding from our earlier conversation was that, you know, **Mr. Wallace was hired, you used the term charity with respect to him working at Tiversa**. I understood that **Mr. Wallace was working primarily on child exploitation or child pornography cases, did a lot of that work from home, and I believe you said you didn't really have a great idea of what he was doing a lot of the time**. So the work that you testified to seems to fall outside the bounds of how you described Mr. Wallace's responsibilities at the company earlier. **Could you help rectify that for us?**

[127] *Id.* at 107-09 (emphasis added).

A. **I don't think it needs rectification**, but this -- maybe you misunderstood what we were saying. Mr. Wallace did do child pornography-type work with the FBI, to the best of my knowledge. **Mr. Wallace, as I already testified to, was an analyst at Tiversa, which then would put him in this information**. He also searched for, on his own, in the time when he was searching his child pornography and other things, he would come up with files. **He would download files outside of our system**, because, as I testified, our system was configured to look for a dynamic signature profile which was specific for each client, which does not just take everything. So therefore, Mr. Wallace would come up with random downloads that, again, because he managed to do the search from end to end, we were confined within a very confined space in the confines of our work product.

Mr. Wallace could put whatever search in at any time. Clearly, as I testified to, I wouldn't have searched for U.S. nuclear information. However, Mr. Wallace apparently came up with this U.S. nuclear information, because, again, he could put whatever search in and see the outcome of it. So therefore, when he came to me and said, here, I have this, this is not through the course of our normal work of Fortune 500 clients. So therefore, he was putting whatever search in any time he wanted to then -- I'm assuming, because then he would come up and provide us these files, and then he also detailed where the file was -- where he downloaded it from**. I had no reason to believe it wasn't true, and I testified to that accordingly**.[128]

Boback reverted again to describe Wallace's role as minimal later in the interview. He stated:

Q. Have you hired anyone to replace Mr. Wallace's work as an analyst for Tiversa?

A. No, he hasn't been an analyst for years, so he hasn't logged in for a long time.

Q. I'm just -- I'm confused about this aspect of it, though. I can't get my head around it --

A. Yeah, okay.

Q. -- because is he doing work just for the FBI, or is he acting as an analyst? What -- I just -- sorry, I keep asking the same question. I want to understand, though.

[128] *Id. at* 110-11 (emphasis added).

> A. Yeah, that's okay. He was not -- in my estimation he was not -- **now, granted nobody watched him**. Like on a daily basis, nobody would say, what is every minute of your day happening? So that was out. **But he was not an analyst. He was not sitting in what the analysts do for years**.
>
> * * *
>
> There was never like one job, specifically that, that's all it was. He could be researching how to delete metadata or do something along those lines. He could be researching other cyber crimes. So he was kind of doing this mix hodgepodge of a bunch of different things.
>
> Q. But he wasn't doing work for Tiversa's other clients?
>
> A. Correct.[129]

As noted above, multiple current and former employees described Boback and Wallace as exceedingly close, both at and outside of work. To the Committee, however, Boback repeatedly characterized Wallace as a dangerous alcoholic. Boback told the Committee that he was aware of Wallace's poor performance and inappropriate behaviors but failed to terminate him for years, even though Tiversa had terminated numerous other employees during the same time period.

When staff questioned Boback's judgment in continuing to employ Wallace in the face of his purported poor performance and erratic behavior, Boback evaded questions with convoluted tangents about how unwell Wallace seemed or the dangers he allegedly posed. He failed to address his own decision-making, instead highlighting at length Wallace's destructive personality.

F. Tiversa's Unseemly Business Practices

1. Tiversa used fearmongering tactics to generate business

From its inception, Tiversa has marketed itself as a vital tool to be wielded against the "scary" and complex world of the peer-to-peer network. Tiversa largely creates revenue through contracts with companies who desire cybersecurity services. To build their brand and generate clientele, Tiversa uses fearmongering tactics by citing stories of the very most sensitive documents on the peer-to-peer falling into the hands of criminals and terrorists.

Sam Hopkins, the creator of Tiversa's technology, gave the Committee examples of the type of information Tiversa had found on the peer-to-peer network. He stated, "I didn't want to

[129] *Id.* at 251-52.

see the stuff, so I just stayed out of it all….There's just scary stuff out there."[130] When asked to explain, Hopkins continued, "Yeah, I mean everyone knows of Snowden. Tiversa has way more than he does and Tiversa has new information on everybody."[131]

Hopkins further described files he had seen during the course of his work with Tiversa:

Q. Let's fast-forward to the discussion of the Marine One schematics. You said at one point that the Marine One schematics were, sort of, the least sensitive thing you've seen. Is that fair?

A. I wouldn't say "least." You know --

Q. One of the least.

A. -- a tax return for somebody is probably the least, but definitely not the scariest. **Scariest would be how to fly a 747 sitting in, you know, the hands of an Arab. You know, that was pretty scary.**

Q. And you've seen that on --

A. Oh, yeah.

Q. -- the peer-to-peer networks?

A. Yeah. **Or, you know, some guy collecting tons of explosive information from the military and also how to tow a boat into the harbor in the Pacific, you know**. Or one of our -- or **all of our bases in the South Pacific, all of their security cameras, exactly where all the gunners are and what the cameras can see and how to gain access, that's pretty scary.**

How to blow up every, you know, big city in America with improvised explosives and exactly what trash cans to stick them in and how to take out bridges, that's pretty scary. Space-based laser stuff, that's pretty scary. Seeing China, Russia, Iran actually grabbing the stuff and seeing it transferred over to them, that was pretty scary.

Q. So who created these documents?

A. Government agencies. Defense contractors.

Q. And these are all in the Tiversa data store?

A. They're out on the peer-to-peer, and Tiversa has some of them.

[130] Hopkins Tr. at 26 (emphasis added).
[131] Hopkins Tr. at 26 (emphasis added).

Q. But everything you just described, is that in the possession of Tiversa in its data store?

A. **That's where I've seen them, yeah. And, I mean, there's millions of files. I mean, it's everything -- I would not be shocked if everybody's information in this room is sitting out there, from your doctors and accountants and, you know, whatnot. It's out there.**

[Att'y] To be clear, when you say in possession of Tiversa, it's not exclusively in the possession of Tiversa. You got it off the Internet.

A. Yeah, it's peer-to-peer. It's probably still out there, and anyone could go and grab it.

Q. But at the time you viewed this information, it had been downloaded by Tiversa.

A. Yeah.

Q. Were these documents marked "classified," do you know?

A. **Oh, yeah. Tiversa is, and peer-to-peer in general, there's tons and tons of classified.** And Tiversa turned over -- Tiversa was in the strange situation, not so much anymore, of that, you know**, they had droves and droves of classified information on all the wars that were going on over in the Middle East. We could see what was happening every day, with all the stuff that was being leaked**. And the government would come every once in a while and get it, and then, you know, it would just sort of disappear, you know[.][132]

Hopkins statements about Tiversa routinely downloading classified information is at odds with what the Committee heard from Tim Hall. Hall told the Committee that much of the information Tiversa provided to him while at NCIS was unclassified.[133] Hall also stated that, since he began working for Tiversa, Tiversa had not determined that it was in the possession of a classified document.[134]

Regardless of how often Tiversa actually downloaded classified information, however, their marketing tactics appear to have worked—Tiversa frequently received press regarding its account of the government security leaks. When Hopkins was interviewed by CNET regarding Tiversa's involvement in the Marine One leak, he stressed the wide-ranging nature of inadvertent leaks on the peer-to-peer, even designating it as "the biggest security problem of all time":

[132] Hopkins Tr. at 97-99 (emphasis added).
[133] Hall Tr. at 39-40.
[134] Hall Tr. at 35.

Q. So your team concluded that the materials fell into the hands of Iran. Is it possible that other actors also are trying to take advantage of similar openings in the system?

A. Heck yeah. Every nation does that. **We see information flying out there to Iran, China, Syria, Qatar--you name it. There's so much out there that sometimes we can't keep up with it.**

Q. I would have assumed military contractors would use more secure networks to communicate.

A. Everybody uses (P2P). Everybody. We see classified information leaking all the time. **When the Iraq war got started, we knew what U.S. troops were doing because G.I.'s who wanted to listen to music would install software on secure computers and it got compromised.**

Q. This is what your company specializes in, obviously, but what's your professional opinion about the extent of this sort of thing?

A. **This is the biggest security problem of all time**. Coming from me, it sounds biased. But you can get 40,000 Social Security numbers out there at the drop of a hat. **We've had people come into our data center and we've shown them things that are out there on P2P and they go away with their minds blown**.[135]

Various outlets portrayed Tiversa as partnering with federal authorities. One outlet wrote, "By the end of [2004], Tiversa was working with the CIA, FBI, Homeland Security, and the U.S. Secret Service."[136] Regarding a WikiLeaks spreadsheet containing potential terrorist targets in California, another outlet wrote, "Asked to aid in the investigation of the leak by U.S. authorities that the company declined to identify, Tiversa found the spreadsheet was inadvertently exposed by a California state employee using a peer-to-peer network in August 2008, more than a year before WikiLeaks posted it."[137]

Tiversa capitalized on this press in their presentations at various conferences and to potential clients.

2. Tiversa systematically mined for files for "potential" clients as a solicitation tactic.

[135] Charles Cooper, *Q&A: Tiversa Co-founder Talks About P2P Leak*, CNet (Mar. 1, 2009), *available at* http://www.cnet.com/news/q-a-tiversa-co-founder-talks-about-p2p-leak/ (emphasis added).
[136] John Foley, *Your Data And The P2P Peril*, InformationWeek (Mar. 13, 2008), *available at* http://www.informationweek.com/your-data-and-the-p2p-peril/d/d-id/1065643?page_number=2. The Committee found many of Tiversa's claims regarding its relationships with federal agencies to be greatly overstated.
[137] Michael Rile, *WikiLeaks May Have Exploited Music Networks to Get Data*, Bloomberg (Jan. 20, 2011), *available at* http://www.bloomberg.com/news/2011-01-20/wikileaks-may-have-exploited-music-photo-networks-to-get-classified-data.html.

A whistleblower told the Committee that Tiversa kept dossiers of information on various companies and executives in an attempt to garner new business. According to the whistleblower, Boback even went so far as to create false documents containing large amounts of sensitive information he obtained through his improper use of a law enforcement database to trick potential clients into purchasing Tiversa's services.

As a matter of practice, Tiversa contacted companies whose documents it found on the peer-to-peer network. Tiversa did so under what it called a "duty of care" policy. However, Tiversa held back critical information from companies whose documents were actually exposed in order to force them to purchase Tiversa's services.

When asked whether Tiversa contacted non-client companies about documents actually exposed on the peer-to-peer network, Boback told the Committee that it did not—that Tiversa only searched the data store for potential clients that had a relationship with Tiversa. He then admitted that Tiversa did in fact "cold call" new clients with documents found on the peer-to-peer network, but stated that it was not a "routine practice." He testified:

> Q. Can you describe circumstances in which you would mine the data store for a potential client?
>
> A. If the client -- if we know we are **-- if we were contacted or we have some relationship with a certain client and we know we are going to see that client**. Prospective clients, yes, prospective clients and the prospectives, it usually starts with a phone call with a prospective client, as any prospective client would start, you have a phone call with the client. You explain to them about the risks of file sharing, the risks of, you know, what this is, and how information can get out this way.
>
> Most people don't understand it, and they say, can you give me an example, so we go into the data store, not into Eagle Vision. We go into the data store and we usually prepare an example sheet of whatever we have in the data store without looking for it; providing that example –
>
> Q. **Have you ever contacted a potential client after mining the data store for information concerning that potential client?**
>
> A. **I think I -- you lost me there.**
>
> Q. Absolutely. **Have you ever looked in the data store for information, found information, and then contacted a potential client?**
>
> [Att'y] **He can't answer. I'm not sure I'm following you. So company X, we want to get them. Let's look for stuff on company X. We call company X?**

Q. Correct.

[Att'y] Okay, do you follow that?

A. Yes. **No, I don't believe so. We may have, but I don't believe so. It is not a routine practice by any means**.[138]

The Committee found, however, that Tiversa routinely "cold called" clients with documents found on the peer-to-peer network. Under the company's "duty of care" policy, Tagliaferri regularly called businesses to alert them to exposed documents. In fact, Tagliaferri called companies nearly every day at some points of his employment with Tiversa.[139] The Committee also spoke with numerous companies that Tiversa contacted seemingly out of the blue about documents it found on the peer-to-peer network. Documents obtained by the Committee further reveal that Tiversa contacted MetLife, NetXert, Open Door, and LabMD regarding use of their services.

[138] Boback Tr. at 146-47 (emphasis added).
[139] *Id.* at 132.

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

From: ifriedman@metlife.com [ifriedman@metlife.com]
Sent: Sunday, July 27, 2008 4:56:27 PM
To: hvaletk@metlife.com
BCC: hvaletk@metlife.com
Subject: Re: IMPORTANT: MetLife Disability Census Found on Web
Attachments: graycol.gif; ecblank.gif; doclink.gif; C2030192.gif; C1078101.gif

Harry - nice work. I thought that might be the case.

Harry Valetk

----- Original Message -----

From: Harry Valetk
Sent: 07/25/2008 05:01 PM EDT
To: Joseph Carroll
Cc: Ira Friedman; Justin Hixson/Leg/MetLife/US@Met[illegible]
Gibbons; Tom Moenan; Meghan Canty
Subject: Re: IMPORTANT: MetLife Disability Census [illegible]

"It seems Traversa [*sic*] solicits business by scanning files online, and bringing them to the company's attention."

Hello All,

I found a July 10th article with Traversa cited in it from a separate, but similar incident involving file-sharing networks. It seems Traversa solicits business by scanning files online, and bringing them to the company's attention.

Just a thought.

==========

A Supreme Court justice's birthday and Social Security number were exposed on the Internet after a McLean, Va., investment firm employee used an online file-sharing network at his office.

Supreme Court Justice Stephen Breyer's birthday and Social Security number, and records for about 2,000 other clients of Wagner Resource Group, were stored in the company's private files. The data breach began late last year and ended shortly after a reader of a blog on washingtonpost.com discovered the information in June on LimeWire.

Wagner hired Tiversa to repair the breach.

Tiversa's chief executive said these breaches are common since many employees and contractors install file-sharing software on office computers. LimeWire, like other file-sharing networks, allow computer users to share files directly by linking computers. But Robert Boback said users don't realize such networks may make all files available, not just music or movie files users hope to share.

"This case is unique because of the high profile of the targets. The individuals on this list are at a very high risk, almost imminent, of identity theft," Boback said.

More than a dozen LimeWire members, including some in Sri Lanka and Colombia, downloaded the personal records from Wagner, according to Tiversa officials. The company was alerted after the blog reader told Security Fix blog employees about the breach and the blog contacted Wagner.

Harry A. Valetk
Corporate Privacy Director
MetLife Privacy Office
212.578.2116 (direct)
Privacy -- Pursue it. Promote it. Protect it. Preserve it.
Joseph Carroll/Pen/MetLife/US

Joseph Carroll/Pen/MetLife/US

07/24/2008 03:09 PM

To Ira Friedman/Leg/MetLife/US@MetLife
cc Harry Valetk/Leg/MetLife/US@MetLife, Justin Hixson/Leg/MetLife/US@MetLife, Larry Wolff/Leg/MetLife/US@MetLife, Michael Fradkin/Ins/MetLife/US@MetLife, Michael Tietz/Ins/MetLife/US@MetLife, Susan

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

----- Forwarded by Michael Fradkin/bts/MetLife/US on 08/02/2008 10:02 PM -----

"Ashish Joshi" <A.Joshi@Lorandoslaw.com>
08/02/2008 09:58 PM

To "Michael Fradkin" <mfradkin@metlife.com>
cc "Justin Hinson" <jhinson@metlife.com>, "Larry Wolff" <lwolff@metlife.com>
Subject Important - Urgent

Michael:

Thank you for your email. I can talk with you and other MetLife pers
a.m. and 11:00 a.m. EST on Monday, August 4, 2008. Monday afternoon d
for me.

As discussed in our teleconference, a few days ago Netxert received a phone call from an agent of Tiversa, Inc. Tiversa's agent informed Netxert that confidential information containing Netxert's employees' personal information (including but not limited to the employees' social security numbers) has been breached and that this information is available on a "P2P server" on the internet. Tiversa's agent refused to disclose the identity or location of this P2P server that contained the personal information of Netxert's employees. However, Tiversa offered to disclose this information, investigate the source of the breach and take remedial steps *if* Netxert agreed to retain Tiversa's services at $495/hour. Netxert informed Tiversa that Netxert needed to see a sample of personal information that was allegedly available on the P2P server and then would take the necessary steps. Tiversa emailed Netxert a MS-Excel file that contains personal & confidential information of Ne employees including their first and last names, social security numbers, date of birth, ge ary details, addresses, etc.

After a preliminary investigation, Netxert has hat there has been no security breach from Netxert's computer systems and/or se tronic file that wa

to Netxert by Tiversa contains metadata that shows MetLife as "author" of the Excel spreadsheet states "MetLife Census for Disability" as its heading. The inform contained in the spreadsheet was sent to MetLife by Netxert's staff at some point i in order to obtain disability insurance. At this stage, it appears that MetLife is the so this security breach.

Frankly, we consider Tiversa's "offer" as nothing short of blackmail. Also, the fact th Tiversa touts itself as MetLife's "vendor" also raises some questions about Tiversa' knowledge and access to this confidential information.

So far, Netxert has not met with the law enforcement authorities to complain about this security breach and Tiversa's tactics. However, soon Netxert will be obligated to (a) inform its employees (residing in several states) and (b) the FBI about this security breach. ***Before*** we take any of the above steps, we want to meet with MetLife's management and discuss these issues and try and work together to resolve this situation. However, time is of the essence in this matter. **We need to act fast**.

Again, I request you to make MetLife's legal personnel (and other necessary personnel) available for a face-to-face meeting on Monday. If you are not able to get everyone together on this short notice, please try and get your in-house lawyers available for a face-to-face meeting on Monday and the rest can join via teleconference. If not Monday, please schedule a meeting on Tuesday – but it is imperative that we have a face-to-face meeting. I do not want to keep discussing this matter via telephone back and forth.

I await your response. If you have any questions, please feel free to reach me on my cell (734-637-7112) over this weekend.

Thank you.

Ashish

ASHISH S. JOSHI
LORANDOS & ASSOCIATES
ATTORNEYS AT LAW
214 N. FOURTH AVENUE
ANN ARBOR, MI 48104
TEL: 734-327-5030
FAX: 734-327-5032
www.lorandoslaw.com

From: Michael Fradkin [mailto:mfradkin@metlife.com]

"a few days ago Netxert received a phone call from an agent of Tiversa, Inc."

"Tiversa offered to disclose this information, investigate the source of the breach and take remedial steps *if* Netxert agreed to retain Tiversa's services at $495/hour."

3. Boback Misrepresented Howard Schmidt's Role in Generating Business Contacts for Tiversa

Tiversa boasts an impressive board of advisors, a corporate governing body separate of the board of directors. The members of the advisory board include Howard Schmidt, General Wesley Clark, Maynard Webb, Larry Ponemon, Michael Dearing, Thomas Keevan, Lynn Reedy, and Patrick Gross.[140] The board purportedly provides "business" and "strategic guidance" to Tiversa.[141] Joel Adams praised the involvement of Tiversa's board. He stated, "Some companies use advisory boards as window dressing…The interaction is minimal, and that type of board isn't worth much. **Tiversa has been able to get its advisers to interact, to participate. When they walk about of a board meeting, they have to-do lists**."[142] Contrary to Adams' praise, however, according to Boback the advisory board met only once, in January 2006. [143]

Instead, Tiversa appears to use the advisory board primarily to solicit clientele. In a bulletin published by Morgan Lewis & Bockius, Boback stated, "when we considered advisers, we asked ourselves, 'Who can provide instructions? Whose credibility can we leverage to get where we need to be?'"[144] The article goes on to note, "Tiversa added the other [advisors], who became stepping stones to clients… and more."[145]

Howard Schmidt serves on Tiversa's board of advisors. During his tenure as advisory board member, he was appointed as the White House Cybersecurity Coordinator under President Obama.[146] Upon his appointment, Schmidt put the options he received from Tiversa into a blind trust. When asked by the Committee about Schmidt's role at Tiversa, Boback expressly denied that Schmidt helped generate business or introduce clients:

Q. Did Mr. Schmidt help generate any business for Tiversa?

A. I don't believe so.

Q. **Did Mr. Schmidt introduce you or anyone else at Tiversa to potential clients?**

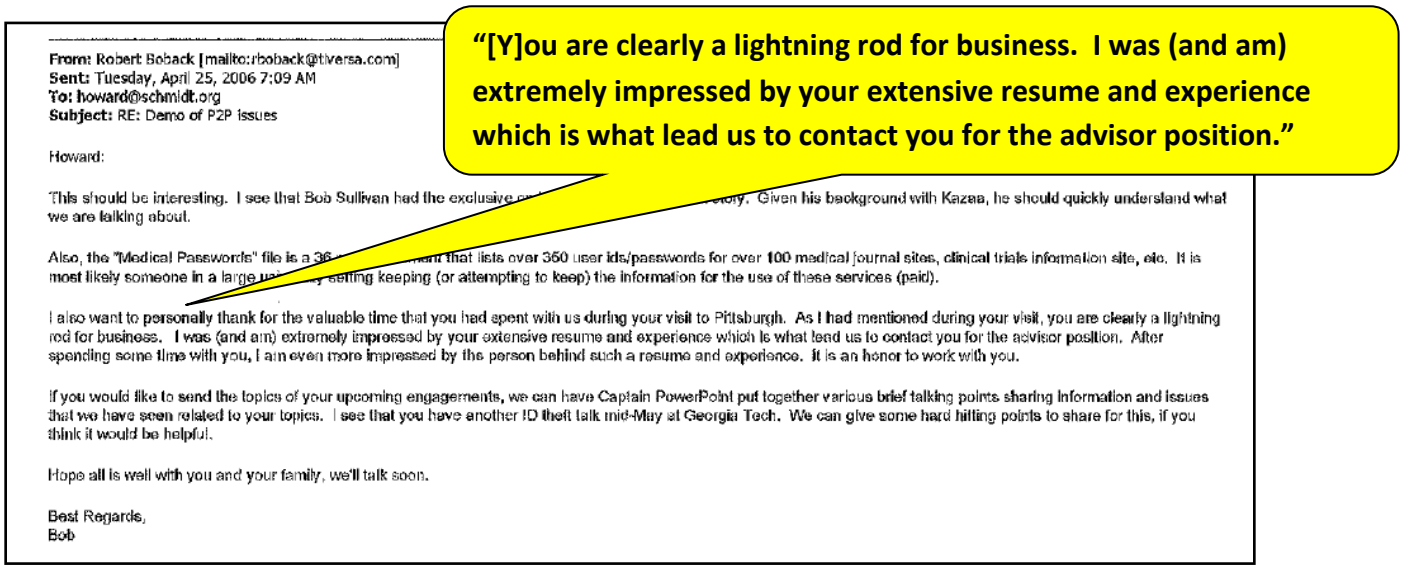
A. **No.** [147]

Contrary to Boback's statement, the Committee has received extensive e-mail correspondence between Boback and Schmidt, where Schmidt systematically introduces Boback

---

[140] Tiversa Advisory Board, Tiversa, *available at* http://tiversa.com/about/advisors.html.
[141] Boback Tr. at 28.
[142] Evan Pattak, *Build a Better Board: See How a Solid Board of Directors Can Poise a Company for Success* 9, Getting It Done II, *available at* http://www.morganlewis.com/pubs/GettingItDone2BuildABetterBoard_TEQ2007i5.pdf (emphasis added) [hereinafter Pattack].
[143] Boback Tr. at 29.
[144] Pattack at 8..
[145] *Id.* (ellipsis in original).
[146] Macon Phillips, *Introducing the New Cybersecurity Coordinator*, The White House Blog (Dec. 22, 2009) http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator.
[147] Boback Tr. at 41.

to potential clients and media contacts. In one e-mail to Schmidt, Boback praised him as "a lightning rod for business": [148]



"[Y]ou are clearly a lightning rod for business. I was (and am) extremely impressed by your extensive resume and experience which is what lead us to contact you for the advisor position."

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Tuesday, April 25, 2006 7:09 AM
To: howard@schmidt.org
Subject: RE: Demo of P2P issues

Howard:

This should be interesting. I see that Bob Sullivan had the exclusive [illegible] story. Given his background with Kazaa, he should quickly understand what we are talking about.

Also, the "Medical Passwords" file is a 36[illegible] that lists over 360 user ids/passwords for over 100 medical journal sites, clinical trials information site, etc. It is most likely someone in a large [illegible] setting keeping (or attempting to keep) the information for the use of these services (paid).

I also want to personally thank for the valuable time that you had spent with us during your visit to Pittsburgh. As I had mentioned during your visit, you are clearly a lightning rod for business. I was (and am) extremely impressed by your extensive resume and experience which is what lead us to contact you for the advisor position. After spending some time with you, I am even more impressed by the person behind such a resume and experience. It is an honor to work with you.

If you would like to send the topics of your upcoming engagements, we can have Captain PowerPoint put together various brief talking points sharing information and issues that we have seen related to your topics. I see that you have another ID theft talk mid-May at Georgia Tech. We can give some hard hitting points to share for this, if you think it would be helpful.

Hope all is well with you and your family, we'll talk soon.

Best Regards,
Bob

Tiversa played in active role in ensuring Schmidt could be an effective advocate. Chris Gormley, copying Boback, gave Schmidt explicit talking points on Tiversa's business model:[149]

[148] TIVERSA-OGR-0017729.
[149] TIVERSA-OGR-0017719.

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

From: Chris Gormley <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=CGORMLEY@tiversa.com>
Sent: Monday, May 1, 2006 12:40 AM
To: 'howard@schmidt.org'
Cc: Robert Boback <rboback@tiversa.com>
Subject: Slides
Attach: Howard043006.ppt

Howard,

Thank you for highlighting the problems we're addressing in your talks over the next 6 days. I've attached some information that may help you on Monday that is focused primarily on the problem in general. I put the files in a neutral file format. The example is a medical one, but it is one that had the least sanitization needed.

What I would like to do is to spend time after today (Monday) working up a more helpful set of slides / presentation to support your other talks this week. I envision the slides supporting two sections:

Section 1: Slides showing the problem in general

Section 2: Modules providing examples for:

1. ID Theft
2. Fraud
3. Regulatory Violations

To support Section 2, I have to sanitize some existing examples. Please let me know if ot ill be helpful in section 2. Also, please let me know what I could do to make the slides I sent to you today more helpful including putting slides into templates tha ur presentations.

Christopher L. Gormley
Chief Operating Officer
Tiversa, Inc.
The Leader in Information Containment Management
Office: 724-940-9030
Fax: 724-940-9033
Mobile: 724-991-3376

This e-mail message and any attachments contain confidential information from Tiversa, Inc. If you are not the intended recipient, you are hereby notified that disclosure, printing, copying, distribution, or the taking of any action in reliance on the contents of this electronic information is strictly prohibited. If you have received this e-mail message in error, please immediately notify the sender by reply message and then delete the electronic message and any attachments.

"Howard, Thank you for highlighting the problems we're addressing in your talks over the next six days. I've attached some information that may help you on Monday…"

Schmidt used these talking points to introduce Boback to potential clients. In June 2006, for example, Schmidt introduced Boback to FAA officials:[150]

From: Howard A. Schmidt <howard@cyber-security.us>
Sent: Saturday, June 3, 2006 5:19 PM
To: Michael F Brown <michael.f.brown@faa.gov>; Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>
Subject: FAA and Data Leakage

Mike,

It was great seeing you at the Aresight meeting and sorry I could not stick around for your presentation.

As I mentioned to you, I have been working with Tiversa and thought that you would find the information that they have found on the P2P networks is unreal. What they have found is not just an errant document here and there but a systemic problem that is found in every sector.

To that end, I would like to introduce you to Bob Boback, the CEO and hopefully you can get a chance to see what they are doing up in Pittsburgh.

Best,
Howard

Sent via BlackBerry - short message and not spell checked.

"I have been working with Tiversa and thought that you would find the information that they have found on the P2P networks is unreal…

To that end, I would like to introduce you to Bob Boback…"

[150] TIVERSA-OGR-0017696.

During the same time, Schmidt introduced Boback to Paypal officials, joking that he hoped Paypal would not hold Schmidt's affiliation against Tiversa:[151]

"I would like to introduce you to Bob Boback…

During a recent call I had with Bob we were talking about the widespread issues around data leakage issues… and he mentioned that there were a number of PayPal related things that his folks had found."

From: Howard A. Schmidt <howard@cyber-security.
Sent: Saturday, June 3, 2006 5:10 PM
To: Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINIS
Barrett <mbarrett@paypal.com>
Subject: "Data Leakage" and PayPal

Michael,

I hope this email finds you well and not too swamped. I would like to introduce you to Bob Boback, CEO of Tiversa a company I started working with on some homeland and defense security issues with.

During a recent call I had with Bob we were talking about the widespread issues around data leakage issues with P2P technology (eDonkey, limewire etc.) and he mentioned that there were a number of PayPal related things that his folks had found. I told him that I would let you know.

For full disclosure, I am their advisory board but hopefully you will not hold that against them. :)

Thanks and seeing what they have found, and continue to find, would be worth your time.

Best,
Howard
Sent via BlackBerry - short message and not spell checked.

"For full disclosure, I am their advisory board but hopefully you will not hold that against them. ☺"

Schmidt also approached Merrill Lynch on behalf of Tiversa, after Boback told him he had unsuccessfully tried to solicit the company:[152]

From: Howard A. Schmidt <howard@schmidt.org>
Sent: Wednesday, April 19, 2006 9:29 AM
To: Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>; 'Basile, Anthony (IS&P)' <anthony_basile@ml.com>
Subject: Introduction as we talked about.

Hello Tony and Bob,

It was good talking with both of you recently and I hope this email finds you both well. Tony, as I mentioned I am on the advisory board of Tiversa and during a recent demonstration for some government related documents the discussion came up about data leakage and financial services. What Bob demonstrated for me was not an isolated document that was found but a widespread systemic leakage problem across ALL sectors, energy, telecom, transportation, financial etc. I think you mentioned that you had heard something about Tiversa but this is something that you have to see yourself to believe.

Thanks and I look forward to catching up next time I am in NY.

Best,
Howard

[151] TIVERSA-OGR-0017697.
[152] second TIVERSA-OGR-0017740

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

From: Howard A. Schmidt <howard@schmidt.org>
Sent: Tuesday, April 11, 2006 11:56 PM
To: Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>
Subject: RE: Merrill Lynch

(IN CONFIDENCE) I am working with them taking a look at their security program for their exec team. I will talk with Anthony Basile who has engaged me. Let me know if you want to send some samples.

Thanks
Howard

-----Original Message-----
From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Tuesday, April 11, 2006 3:02 PM
To: howard@schmidt.org
Subject: Re: Merrill Lynch

Hi Howard,
ML is one of the worst when it comes to leakage. We have made initial contact but have been stopped by a mid level IT individual named Swati Dutta Roy. They don't understand the problem. Any assistance that you can lend would be much appreciated.
Thanks
Bob

-----Original Message-----

From: "Howard A. Schmidt" <howard@cyber-security.us>
Subj: Merrill Lynch
Date: Tue Apr 11, 2006 11:44 am
Size: 227 bytes
To: "Robert Boback" <rboback@tiversa.com>

Hi Bob,

I have a consulting job with ML and as I talk with them I wanted to give them some insights into if they were leaking. Have you seen anything?

Thanks
Howard
Sent via BlackBerry - short message and not spell checked.

"(IN CONFIDENCE) I am working with them taking a look at their security program… I will talk with [ML official] who has engaged me."

"We have made initial contact but have been stopped by a mid level IT individual… Any assistance that you can lend would be much appreciated."

Tiversa also leveraged Schmidt's reputation for publicity. Schmidt contacted news outlets on Tiversa's behalf:[153]

From: Howard A. Schmidt [mailto:howard@schmidt.org]
Sent: Monday, April 24, 2006 11:19 PM
To: Robert Boback; 'Bob Sullivan (MSNBC-JV)'
Subject: Demo of P2P Issues

Bob (and Bob, MSNBC) ☺ ,

Bob Sullivan and I both spoke at an event with the AG for Ohio today on their ID Theft program. After the lunch, I talked with Bob about what you were doing and some of the really dangerous things that you showed me. I also explained to him that you did not want to alienate potential customers and that it would be counter productive to "report" on who had problems (everyone) but it might be a good way for Bob to raise the awareness. He did a story a while back around Kazzaa but I do not think he has seen anything like you showed me.

To that end, I would like to introduce you to each other to see what you can work out. Please let me know if there is anything I can do to help.

Best,
Howard

"I would like to introduce you to each other o see what you can work out."

[153] TIVERSA-OGR-0017729

The Committee found that, contrary to Boback's statements about Schmidt's role at Tiversa, Schmidt actively sought out contracts and potential clients for the company. This is yet another example of Boback providing false information during the course of this investigation.

4. Boback Misrepresented Information about Tiversa's Capabilities to Clients

According to a former Tiversa employee, Boback had a propensity to exaggerate, or even lie at times. Gormley stated, "the perception at least from what I remember internally was that there was a tendency to exaggerate or at least misrepresent… what was going on at the time."[154] Specifically, the feeling among some employees was that Boback's statements were "60 percent, you know, bullshit; 30 percent not true; and 10 percent truth, I guess, as far as like a representation of the facts."[155]

Gormley recalled a specific instance in which Boback misrepresented facts in meeting with a client:

> Q. When you say "third parties," do you mean potential clients?
>
> A. I remember the incidents. I mean, one was an existing investor, a limited partner within Adams Capital, came into the meeting, into a discussion, and **the number of employees and the revenues of our companies were overstated at the time**.
>
> The other was, well, to General Wesley Clark and Yahoo around **whether we were profitable or not**. And, again, you know, at the time, we were profitable for one quarter, but we weren't profitable for an entire year. I looked at that as misrepresenting that we're profitable, but you could argue that we were profitable for one quarter.
>
> There were also too many employees attributed to a potential acquirer named SecureWorks. That was later corrected, of course, in diligence, because you know how many employees you have, right?
>
> And those are some of the incidences I remember. And then -- so those are some -- I'm just trying to remember some of the other major areas.
>
> Q. Sir, did you ever confront Mr. Boback about these misrepresentations?

[154] Gormley Tr. at 131-32.
[155] *Id.* at 131, 136.

A. Yeah, I mean, I told him, you can't do that, they're going to -- particularly in the case of potential acquirers, they're going to find out. I mean, let's not say that. We lose credibility in those instances.

The case of this limited partner, the individual on the other end of the table was someone who friends of mine knew, so I felt personally at odds.

Q. And this is the gentleman from Adams Capital?

A. No, it's a limited partner, who was an investor in Adams Capital that came in to see essentially what Adams Capital was investing in. So, I mean, to me, the risks there were lower, because they had already invested. But we can't not state -- now, again, there's all different ways of viewing this. I mean, are you counting every single part-time potential person? Are you counting -- I mean, **but I recall it being an order of magnitude different**; it wasn't close.

So that was one incidence -- set of instances that I remember.[156]

In another instance, Boback represented to a potential client that he had a close personal relationship with the FBI, implying retaliatory action if the client did not take action:

> **[I]n the discussion, Bob mentioned very lightly, but it stood out that he knows people at the local FBI office. And the veiled implication was that continue with monitoring, or else that FBI office might get wind of this.**[157]

During the course of its investigation, the Committee routinely found that it could not take information provided by Tiversa at face value—and statements made by former employees indicate that clients and potential clients could not do the same. The Committee found that Boback's statements about Tiversa's technological capabilities simply did not match what it found in the documents and testimony, Boback created a hostile work environment, withheld the nature of his relationship with Richard Wallace from the Committee, and created a culture at Tiversa based on a series of unseemly business practices. The Committee found that information provided by Tiversa—such as that on the Marine One leak—not only could not be verified, but at times appeared to be outright false. Given all the Committee has learned about Boback and Tiversa, the extent of its relationship with the Federal Trade Commission is extremely concerning.

V. Tiversa's Relationship with the Federal Trade Commission

[156] *Id.* at 27-29 (emphasis added).
[157] Gormley Tr. at 132-33 (emphasis added).

Tiversa's interactions with the FTC raise questions about the propriety of the relationship. Both Tiversa and the FTC have characterized the relationship as nominal. Overwhelming evidence produced to the Committee, however, demonstrates mutually-beneficial collaboration, wherein the FTC obtained information validated its regulatory authority, and Tiversa gained an ally in a powerful federal agency that provided actionable information that it exploited for monetary gain. Unfortunately, this relationship existed at the expense of good government.

The FTC accepted information from Tiversa through a shell organization without questioning the motives or reason for the third party, or, significantly, the veracity of the underlying information. The FTC's motives for blindly accepting this information are unclear.

In addition, Tiversa's involvement with LabMD, a medical testing laboratory based in Atlanta, Georgia, raises questions. Not only does LabMD's story offer a case study illustrating Tiversa's coercive business practices and relationship with the FTC, but information the Committee obtained shows that Boback lied about material information in the case, which ultimately led to the shuttering of LabMD.

According to a whistleblower, Tiversa withheld from the FTC information about its clients that had data breaches while providing information for companies that rejected the offer to buy Tiversa's services. According to the whistleblower, the FTC blindly trusted Tiversa's data and took only nominal steps to verify the information before embarking on the dissemination of warning letters and enforcement actions. Documents provided by the Federal Trade Commission also indicate the limited steps taken to verify information provided by Tiversa.

A. Tiversa misrepresented the extent of its relationship with the FTC to the Committee

On July 9, 2009, weeks before Tiversa testified before this Committee for the second time, the FTC sent a civil investigative demand to an entity Tiversa created called the Privacy Institute.[158] Tiversa responded promptly, passing documents and information about peer-to-peer breaches at nearly 100 companies through the Privacy Institute, which the Committee learned was created for the sole purpose of funneling information to the FTC pursuant to the CID. When the Committee asked Boback about Tiversa's relationship with the FTC, however, he painted a picture of a government agency bullying a small company. He testified:

> We wanted to create separation, as we felt we were being bullied by the FTC into having to provide information to—a small company having to be forced to provide information.
>
> **Because in July of 2009, I testified before this committee and then I was bullied by the FTC the very following month, in my opinion, in providing that information.**[159]

[158] Letter from Reginald Brown, Att'y, Tiversa to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (July 22, 2014).
[159] Boback Tr., at 43 (emphasis added).

Boback reiterated this sentiment by stating:

> And we felt -- frankly, as I mentioned, **we felt bullied or trapped to where we were saying I had no choice but to comply with something that was no benefit to Tiversa, was time-consuming, was costly to a small company**, kind of like I feel today.[160]

Boback asserted that Tiversa "denied" the FTC's request for information, and, under threat of a civil investigation demand (CID), Tiversa was compelled to provide information to the FTC.[161]

Consistent with his stated reluctance to cooperate with the agency, Boback described his contacts with the FTC as very limited. He testified he only knew one person at the FTC—Alain Sheer—and that he only interacted with Sheer on four occasions.[162] According to Boback, Sheer contacted him after the July 2009 Oversight hearing to set up a visit to Tiversa.[163] A second contact occurred when Sheer visited Tiversa in August 2009. Boback testified about the FTC's visit to Tiversa:

> So he came to Tiversa. They looked in our data center. They went in and said, "We'd like to talk about having" -- we met in our conference room and they said, "We'd like to talk about getting the copies of the information that you provided to House Oversight."
>
> They went into our data center to look at it. And he said, "I want these copy" -- "I need these printed out for us. I need these sent to us." And we said, "We don't send any information from our data center. Our data store is our data store. That is sacrosanct to us. So that's it." And they said, "Well, we're going to need to get this information, and we can use the CID, if necessary." We didn't know what a CID was. He said, "Civil investigative demand, similar to a subpoena. We're going to get the information." And we went, "Oh, no."[164]

Yet, by the time this meeting took place in August 2009, Tiversa had already received the CID. It is unclear why the FTC would threaten Tiversa with a CID a month after the CID was issued to the Privacy Institute.

Boback met with Sheer for the third time in Washington, D.C., after the Privacy Institute responded to the FTC's CID with information it in turn obtained from Tiversa.[165] Then,

---

[160] *Id.* at 218 (emphasis added).
[161] *Id.* at 43.
[162] *Id.* at 188 (Q: "What other attorneys at the FTC, besides Mr. Sheer, have you interacted with?" A: "There were two other attorneys at my deposition in November, but I don't recall their names… I don't know anyone at the—the only person I 'know' at the FTC is Mr. Sheer.").
[163] *Id.* at 184-85.
[164] *Id.* at 185-186.
[165] 186. As discussed below, representatives of the FTC do not recall meeting with Boback in Washington, D.C. It is not clear whether or not this meeting actually took place.

according to Boback, he did not have contact with Sheer until Sheer took his deposition in November 2013.[166] The fourth meeting occurred in June 2014—just before the Committee interviewed Boback.[167]

B. The FTC misrepresented the extent of its relationship with Tiversa to the Committee.

The FTC told the Committee that it had limited contact with Tiversa. Representatives from the Division of Privacy and Identity Protection of the Bureau of Consumer Protection told the Committee that the FTC first contacted Tiversa around the time of the July 2009 hearing.[168] FTC officials stated they found Tiversa to be a credible source of information, in large part, because of Boback's previous testimony before the House Oversight Committee.[169]

According to the FTC, after Tiversa sent the information responsive to the CID through the Privacy Institute, all subsequent contacts with Tiversa took the form of clarifying questions about the information provided by Tiversa.[170] Alain Sheer and Kristen Cohen made these calls.[171] As described above, FTC officials also recalled a meeting at Tiversa's offices in 2009, although they could not remember the details.[172] FTC officials did not recall any other meetings with Tiversa. Sheer in particular did not recall meeting with Tiversa in Washington, D.C.[173]

E-mails produced to the Committee—including from entities other than Tiversa—show a much more cooperative relationship between Tiversa and the FTC. Contrary to the assertions Boback made during his transcribed interview as well as those FTC officials made, documents show Tiversa's relationship with the FTC began in the fall of 2007. In October 2007, Boback participated in a conference call with FTC officials.[174] In December 2007, Boback provided documents to the FTC.[175] In June 2008, FTC attorney Carl Settlemyer thanked Boback for his "cooperation and insights into the area of inadvertent file sharing over P2P networks," and notified him that "confidential" information Tiversa provided to the FTC related to earlier Committee hearings on P2P networks would be produced to the Oversight Committee.[176] In

---

[166] *Id.*
[167] *Id.*
[168] Briefing by FTC officials to H. Comm. on Oversight & Gov't Reform Staff (Sept. 9, 2014) [hereinafter FTC Briefing].
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] E-mail from Robert Boback to Carl Settlemyer, Att'y, Fed. Trade Comm'n (Oct. 22, 2007 3:25 p.m.) [TIVERSA-OGR-0000071]; GoToMeeting Invitation—FTC Meeting 10:30 a.m. to 11:30 a.m.
[175] E-mail from Robert Boback, CEO, Tiversa to Carl Settlemyer, Att'y, Fed. Trade Comm'n (Dec. 19, 2007 3:08 p.m.)[TIVERSA-OGR-0000065]; E-mail from Carl Settlemyer, Att'y, Fed. Trade Comm'n (June 25, 2008 12:13 p.m.) [TIVERSA-OGR-0000063].
[176] E-mail from Carl Settlemyer to Robert Boback (June 25, 2008 12:13 p.m.) [TIVERSA-OGR-0000063] (attached letter from Carl Settlemyer, Att'y, Fed. Trade Comm'n, to Robert Boback (June 25, 2008) [TIVERSA-OGR-0000064]).

March 2009, Boback again participated in a conference call with the FTC.[177] Days later, Boback bragged about the call: [178]

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, March 09, 2009 8:59 AM
To: Kline, Eric D.; Todd Davis
Subject: RE: Tiversa comparison

Todd,

I'm an in the office today if you want to discuss this after you have had a chance to review. I also wanted to give you an update on the great call that I had with the FTC on ID theft issues.

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

Personnel from the FTC's Division of Privacy and Identity Protection told the Committee that Tiversa's contacts with the FTC prior to the July 2009 hearing took place with a different division of the FTC.[179] Yet, Alain Sheer was included on e-mails with Boback requesting information about a recent Tiversa press release and scheduling the March 5, 2009, conference call[180]—the same call that Boback boasted about days later.

Tiversa's phone records are also telling of the company's relationship with the FTC. They indicate that Tiversa employees placed two phone calls to FTC attorney Laura Vandruff in June 2008, and that in the four months leading up to the July 2009 Oversight Committee hearing, Tiversa employees called Alain Sheer at his FTC office on 21 occasions.[181] Documents show that Boback was one of the FTC's main contacts at Tiversa prior to July 2009.

Regular phone calls between Tiversa and the FTC took place between August 2009, when Tiversa provided information to the FTC, and January 19, 2010, when the FTC sent letters to nearly all of the companies Tiversa turned over to the FTC. During these months, Tiversa

[177] E-mail from Robert Boback to Carl Settlemyer, Att'y, Fed. Trade Comm'n (Mar. 4, 2009 1:55 p.m.) [TIVERSA-OGR-0000052].
[178] E-mail from Robert Boback to Todd Davis, CEO of LifeLock, and Eric Kline (Mar. 9, 2009 8:59 a.m.) [LLOCK-OGR-000147]. Tiversa failed to produce this email to the Committee.
[179] FTC Briefing.
[180] *See* e-mail from Carl Settlemyer, Att'y, Fed. Trade Comm'n, to Robert Boback, CEO, Tiversa, Stacey Ferguson, Alain Sheer, & Richard Quaresima, Fed. Trade Comm'n (Mar. 4, 2009 5:25 p.m.) [TIVERSA-OGR-0000052-54].
[181] Consolidated Comm'ns, Invoice P724940903002007081 6TIVERSA_INC [hereinafter Tiversa Phone Records].

employees called Alain Sheer 34 times.[182] The FTC represented to the Committee that only a handful of phone calls ever took place. Tiversa also represented to the Committee that the relationship between Tiversa and the FTC was nominal, and produced few documents indicating any ongoing contract with the FTC after July 2009, let alone this many interactions. The phone records stand in stark contrast to this assessment.

As discussed below, Tiversa used its advanced knowledge of FTC regulatory actions for its own commercial gain.

C. The FTC failed to question Tiversa's creation of a dubious shell organization, the Privacy Institute, to funnel information to the FTC

Despite the friendly relationship between Tiversa and the FTC, Tiversa asked the FTC to accept documents from a company it created for the sole purpose of responding to the FTC—the Privacy Institute. The certificate of incorporation was filed in Delaware on June 3, 2009.[183] Boback testified about Tiversa's purpose in creating the Privacy Institute:

> Q. Mr. Boback, what is The Privacy Institute?
>
> A. Privacy Institute is an organization our lawyers set up.
>
> Q. For what purpose?
>
> A. Well, was it originally? I mean, it was –
>
> Q. For what purpose was it set up?
>
> A. Right. It was set up to provide some separation from Tiversa from getting a civil investigative demand at Tiversa, primarily. And, secondarily, it was going to be used as a nonprofit, potentially, but it never did manifest.[184]

* * *

[182] *Id.*

[183] Sec'y of State, State of Del., Div. of Corps., Certificate of Incorporation, No. 4694728 (June 3, 2009) . [hereinafter Certificate of Incorporation]. The Privacy Institute was dissolved on June 18, 2013. On the certificate of dissolution, the address for Brian Tarquinio is that of Boback's uncle. In a deposition taken just days after the Committee's transcribed interview, Boback testified that he did not know why his uncle's address was used on the certificate of dissolution. Deposition of Robert Boback, In the matter of LabMD, No. 9357 (June 7, 2014) at 38. Tarquinio also testified that he did not know why the address of Boback's uncle was listed as his own on this document. Tarquinio Tr. at 23-24. Upon learning this information, the Committee asked Boback why the address of his uncle was used on this document. Letter from Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform, to Robert Boback, CEO, Tiversa (June 23, 2014). One month later, Boback, through his counsel, answered that he did not recall. Letter from Reginald Brown, Att'y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (July 23, 2014).

[184] Boback Tr., at 42.

> A. I don't know if it was their idea or our idea. We wanted to create separation, as we felt we were being bullied by the FTC into having to provide information to -- a small company having to be forced to provide information.
>
> Because in July of 2009, I testified before this committee and then I was bullied by the FTC the very following month, in my opinion, in providing that information.
>
> When we denied providing them information, all of a sudden we were told that, "You have no -- you have no right to deny it, and here's a civil investigative demand that is coming for this."
>
> And we talked to them and said, "We are in acquisition talks at Tiversa and the last thing we want to have is some Federal subpoena or civil investigative demand coming to us."
> So our lawyers, in talking to the FTC, they said, "Fine. We'll send this civil investigative demand to this other company, this Privacy Institute, and do it that way."[185]

In the same interview, Boback stressed again that the "singular purpose" of the Privacy Institute was to maintain distance between Tiversa and the FTC's CID. Boback stated:

> Q. How would you describe the relationship between the Privacy Institute and Tiversa?
>
> A. It was one singular purpose that was to make sure or try to do whatever we could so that the FTC did not send a CID, the civil investigative demand, to Tiversa. And that was the only option that our attorneys came up with and the FTC was okay with. So -- or, I don't know if they were okay with it. If they were okay with it, they did it.[186]

Boback asked Brian Tarquinio, his financial advisor, to be the President of the Privacy Institute. Tarquinio accepted the requested as a "favor" to Boback.[187] Tarquinio had a different understanding of the purpose of the Privacy Institute. Tarquinio stated:

> Q. Could you describe for us what the Privacy Institute is?
>
> A. I don't think it's anything at this point.
>
> Q. How about what it was?

---

[185] *Id.* at 43.
[186] *Id.* at 48.
[187] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Brian Tarquinio (Sept. 5, 2014), at 57 [hereinafter Tarquinio Tr.].

A. Sure. To my best recollection, **it was an entity that was established to take bids for either part or all of Tiversa if a company wanted to purchase them.**[188]

* * *

A. Sure. My recollection is **it was set up because at the time there were companies that were interested in potentially purchasing Tiversa, and it would be a separate entity to take those bids.**[189]

Tarquinio's understanding of the purpose of the Privacy Institute came directly from Boback:

[Att'y] Why don't you just explain how it came to your attention, what your involvement was, and then they'll have follow-ups.

A. Sure. Mr. Boback came to me and said, we have a company, and at the time I believe it was LifeLock, who was interested in purchasing, you know, some part of Tiversa, which I was aware of. **And he said, we want to create an entity separate from Tiversa to accept those bids, so it is not on our corporate side of everything.** We would like to see if you would be, you know, the head of the Privacy Institute. And as a friend, it seemed pretty reasonable. I said to him, sure, if I get approval [from my employer], fine, glad to.[190]

According to Tarquinio, Boback did not inform Tarquinio that the Privacy Institute was set up to transmit information to the FTC. In fact, Boback did not even mention the involvement of the FTC to Tarquinio. Tarquinio stated:

Q. Concurrent with your involvement in the Privacy Institute, were you told that the creation of the Privacy Institute had anything to do with the FTC's interactions with Tiversa?

A. At that time, no. I had no knowledge of the FTC's interaction with Tiversa.[191]

Tarquinio had no knowledge that the Privacy Institute had ever transmitted information to any government entity,[192] and only recently learned of the Privacy Institute's connection to the FTC:

---

[188] *Id.* at 16.
[189] *Id.* at 17.
[190] *Id.* at 20.
[191] *Id.* at 21.
[192] *Id.* at 22.

> Q. At what point in time did you learn that the Privacy Institute was somehow connected to the FTC? Was it during the course of your preparation for today?
>
> A. Yes, ma'am.[193]

Tarquinio's testimony contradicts Boback's explanation of the Privacy Institute's creation, and raises questions regarding the true purpose and activities of the Institute, which remain unknown.

Regardless of the reasons that Boback created the Privacy Institute, it is not in dispute that Tiversa used the Privacy Institute to send information to the FTC. The FTC did not question Tiversa's use of the Privacy Institute, and did not know that the Privacy Institute was set up solely to respond to the FTC's request for information.[194] FTC officials clearly knew that the information was, in fact, coming from Tiversa, despite the use of the Privacy Institute.[195] The FTC admitted that the use of Tiversa's information was unusual relative to standard agency operating procedures for enforcement measures.[196]

FTC officials relied heavily on Tiversa's "credible" reputation in "self-verifying" the produced information.[197] The FTC explained to the Committee the steps it took in "self-verifying" the information:

- Tiversa, through the Privacy Institute, certified the information provided under penalty of perjury.
- FTC employees looked up the IP addresses provided by Tiversa to determine if the IP address was affiliated with the company.
- FTC employees looked at the metadata of the documents, when provided, to determine the author or the document.
- FTC employees performed "some" searches on the peer-to-peer networks, both for company names and specific documents. The FTC independently found only one of the files Tiversa submitted on the peer-to-peer network.[198]

Ultimately, outside of some minimal work verifying IP addresses and looking at metadata, the FTC relied entirely on the list of companies and documents Tiversa provided. Of the 88 companies Tiversa submitted to the FTC, the agency sent warning letters to 63 companies, and opened investigations into 9 companies.[199] The FTC also issued a press release on the letters

---

[193] *Id.* at 22-23.
[194] FTC Briefing.
[195] *Id.*
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] [FTC_PROD16732-16964].

and received considerable media exposure for its new work related to data security. According to the FTC, this was the only time it obtained information from Tiversa.

The FTC further explained that it only needs "reason to believe" that a company is failing to adhere to appropriate data security standards before sending a warning letter or issuing a complaint. The agency was comfortable with the extent of the "self-verifying" steps it took before sending warning letters and opening investigations into nearly 100 companies. The FTC categorically denied to the Committee that it gave Tiversa notice that it would be using the information in letters to companies. Documents the Committee obtained during the course of this investigation suggest otherwise.

D. Tiversa manipulated advanced, non-public, knowledge of FTC regulatory actions for profit

Tiversa had advanced knowledge that the FTC intended to pursue regulatory actions against many of the companies it turned over to the Privacy Institute in response to the CID. FTC officials maintained to the Committee that no one at the FTC provided advance information of the January 2010 regulatory actions to Tiversa.[200] Tiversa did not produce the overwhelming majority of the documents indicating Tiversa's intention to profit off the FTC's actions. Tiversa failed to produce these documents despite the fact that they were clearly responsive to both the original subpoena, and the search terms provided by Committee staff.[201] The Committee obtained these documents from other sources.

Armed with non-public knowledge of these impending actions, Tiversa maneuvered to position itself to profit from the FTC's actions. In the fall of 2009, Boback began working with LifeLock, a major partner of Tiversa and Tiversa's largest source of income, to send letters to the companies that would be contacted by the FTC—the very companies that Tiversa turned over to the FTC. In October 2009, Boback e-mailed senior LifeLock executives about the impending FTC investigations:[202]

[200] FTC Briefing..
[201] Subpoena from H. Comm on Oversight & Gov't Reform to Tiversa, Inc. (June 3, 2014). The subpoena requires production of "all documents and communications referring or relating to work Tiversa, Inc. performed for the Federal Trade Commission. *Id*. The Committee further provided the search terms "FTC" and "Federal /2 trade /2 commission".
[202] E-mail from Robert Boback to Mike Prusinski, Todd Davis, and Clarissa Cerda (Oct. 26, 2009 7:37 a.m.) [LLOCK-OGR-0002009].

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, October 26, 2009 7:37 AM
To: Mike Prusinski; Todd Davis; Clarissa Cerda
Subject: RE: 60 minutes

As soon as I get the OK from the FBI, we will be off an running. We have some huge rings that we are tracking right now but I can't discuss as they are open investigations. We hired a new guy that came from the Secret Service to help us address these crimes.

Also, there was a breach in House Ethics via P2P that the Washington Post will be writing a story about this week or next. Should be interesting...

And....the FTC is preparing the federal cases against 100 or so companies that have breached consumers information via P2P. This is a huge increase for them since they have only prosecuted 25 cases since 2001. The Washington Post is already planning on writing a big expose on that and they plan to name companies in an effort to shame them into properly addressing this for the individuals exposed.....ie buy LL. :-) There are about 600-700K individuals on those lists, therefore if we time things right, LL can have a huge upswing in members AND LL will have pricing power over the companies that leaked the information. Since LL is still the only company that can offer P2P remediation, you will be the only choice for the solution. :-)

I saw the settlement of the Experian suit.....they mus[illegible] seen that Todd on the stand and Clarissa on a cross examination would not be beneficial to their [illegible]viability.....

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

"the FTC is preparing the federal cases against 100 or so companies that have breached consumers information via P2P"

The "100 or so companies that have breached consumers [*sic*] information via P2P" were the same companies that Tiversa itself reported to the FTC. Boback further explained that the *Washington Post* planned to "shame" companies into addressing the problem, and that the upcoming FTC investigations presented a unique opportunity for LifeLock and Tiversa to profit.[203]

Boback's scheme to profit from the FTC investigations took shape in the coming weeks. In early October 2009, Boback advised LifeLock that "the FTC letters did not go out yet so the companies will not know what you are talking about……yet."[204] He further advised that LifeLock should "be solo" and "suggest Tiversa if asked by the company."[205]

[203] *Id*.
[204] E-mail from Robert Boback to Anthony Hesano, LifeLock (Oct. 6, 2009 8:40 a.m.) [LLOCK-OGR-0001929]. Tiversa failed to produce this e-mail to the Committee.
[205] *Id*.

----- Original Message -----
From: Robert Boback <rboback@tiversa.com>
To: Anthony Hesano
Sent: Tue Oct 06 08:40:21 2009
Subject: RE: FTC letter

I agree with your approach. The FTC letters did not go out yet so the companies will not know what you will be talking about.....yet. I think that it LL should be solo on this.....you could always suggest Tiversa if asked by the company. :-)

It was great to catch up with you and Ally as w I understand that Jacque is in town this week. Brian is a totally straight up guy that lutely not try anything out of line, or even close to any line.....and I mean that.

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

"The FTC letters did not go out yet so the companies will not know what you will be talking about...yet. I that that… LL should be solo on this… you could always suggest Tiversa if asked by the company. ☺"

The following month, Tiversa and LifeLock's strategy with respect to the as-yet-unannounced FTC investigations became clear. In a November 3, 2009, e-mail, a LifeLock employee stated that he "spoke with Bob" about repositioning the letter.[206] He described the attached version as one that will "get the response we are looking for without overplaying our cards." Another LifeLock employee responded, stating, "As mentioned, Clarissa has stopped this pending the FTC but our strategy is to send a letter similar to the one outline[d] along with the breach brochure."[207] A later e-mail describes the revised strategy:[208]

[206] E-mail from Gary Woods to Steve McGrady, Eric Warbasse, and Chris Miller (Nov. 3, 2009, 10:35 a.m.) [LLOCK-OGR-0002044].
[207] E-mail from Steve McGrady to Gary Woods, Eric Warbasse, Chris Miller, and Austin Colcord (Nov. 3, 2009 12:00 p.m.) [LLOCK-OGR-0002043-2044].
[208] E-mail from Gary Woods to Austin Colcord and Chris Miller (Nov. 3, 2009 2:25 p.m.) [LLOCK-OGR-0002043].

EMBARGOED UNTIL AFTER THE TESTIMON

From: Gary Woods
Sent: Tuesday, November 03, 2009 2:25 PM
To: Austin Colcord; Chris Miller
Cc: Anthony Hesano; Eric Warbasse; Steve McGrady
Subject: FW: LifeLock Breach Services - intro letter

Austin & Chris

I re-wrote the letter and believe it is on target – and generic enough that Legal is not going to have any issue. I spoke with Eric & Austin about it and now I just need Chris to have Legal approve the verbiage.

Key points:
- No FTC reference
- No Tiversa reference
- No P2P reference

This is solely to make these accounts aware of LifeLock so when they fully realize the need to respond to a data breach – they think of LifeLock first and have our contact information to reach out and partner with us. I'm sure based on discussions with Bob that Tiversa will also be involved with these accounts and will reinforce their need to provide a LL solution in their breach compliance letter to affected individuals.

Thanks for your help,

Gary

"Key points:

- **No FTC reference**
- **No Tiversa reference**
- **No P2P reference"**

As discussed, the draft letter, as provided to Boback on November 3, 2009, contains no reference to the FTC, no reference to Tiversa, and no reference to the peer-to-peer networks.[209]

On February 22, 2010, the FTC announced that it notified "almost 100 organizations" about data breaches that occurred on peer-to-peer file sharing networks, and opened non-public investigations into several other companies.[210] Boback sent the link to executives at LifeLock:[211]

From: Robert Boback
To: Gary Woods; Todd Davis; Mike Prusinski
Sent: Mon Feb 22 09:30:18 2010
Subject: FTC press release

Guys,

Check out this link.....then ask yourself who knows what's going on?!?!?!?! :-)

http://www.ftc.gov/opa/2010/02/p2palert.shtm

Best,
Bob

Robert Boback
Chief Executive Officer

1

[209] Draft Letter, LifeLock (undated) [LLOCK-OGR-0002045].
[210] Press Release, FTC, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* http://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe
[211] E-mail from Robert Boback to Gary Woods, Todd Davis, and Mike Prusinski (Feb. 22, 2010 9:30 a.m.) [LLOCK-OGR-0002375].

LifeLock responded, "Once again you guys are at the top of the food chain. Any problem with us pushing this with media and using you?"[212] Boback promptly replied, "No problem."[213]

In an interview with *Computerworld* days after the FTC press release, Boback stated, "We were happy to see that the FTC [has] finally started recognizing that P2P is a main source for criminals to gain access to consumer's personally identifiable information for ID theft and fraud."[214] Boback further stated that complying with the FTC's request for information could be "extensive and cumbersome," and that 14 of the companies the FTC contacted had already contacted Tiversa for help.[215] The *Computerworld* article does not mention that Tiversa acted as the primary source for the FTC's enforcement actions announced in February 2010.[216]

When asked about the propriety of Tiversa seeking to profit from its dealing with the FTC, FTC attorney Alain Sheer stated that it was routine for the FTC to make clear to third parties that the information was not public.

> Q. In the course of your interactions with Tiversa in the pre-complaint period, did you or one of your colleagues ever tell Tiversa not to discuss the conversations that the FTC and Tiversa were having with third parties?
>
> A. It is routine for Commission staff to ask entities that are providing information to keep the information confidential.
>
> Q. Do you recall making that specific request to Tiversa? A I don't recall it. Q It would've been your general practice or your colleagues' general practice to make that request? A Yes.[217]

Sheer further testified that he was unaware of Tiversa seeking to profit off of the information provided to the FTC until shown documents produced to the Committee and that the scheme with Lifelock was concerning.

> Q. Does it concern you that Mr. Boback seems to have obtained some sort of information about what the FTC planned to do as early as October 26, 2009?
>
> A. The company provided information about roughly 100 companies when they looked at it. They are well aware of what it is they gave to us. So is it a concern?

---

[212] E-mail from Mike Prusinski to Robert Boback (Feb. 22, 2010 11:47 a.m.) [LLOCK-OGR-0002375].
[213] E-mail from Robert Boback to Mike Prusinski (Feb. 22, 2010 10:00 a.m.) [LLOCK-OGR-002375].
[214] Jaikumar Vijayan, *FTC Questions Firms Being Probed for P2P Breaches*, TECHWORLD (Feb. 26, 2010), http://news.techworld.com/security/3213712/ftc-questions-firms-being-probed-for-p2p-breaches/?olo=rss
[215] *Id*.
[216] Tiversa informed the Committee that it had prior business relationships with 11 companies whose information was included in response to the CID. This conflicts with statements Boback made in the *Computerworld* interview that "14 of the companies contacted over the leaks have already contacted Tiversa for help" and that "all but two of those have CIDs." Not only is the number of companies with contracts with Tiversa inconsistent, but many of the companies that received CIDs from the FTC did not, in fact, have contracts with Tiversa.
[217] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer, Fed. Trade Comm'n, Transcript at 94 (Oct. 9, 2014) (hereinafter Sheer Tr.).

> Yes. I'd like it to be kept confidential. That's the point of asking for it to be kept confidential.[218]

Troublingly, despite Tiversa's close relationship with Lifelock, a company that was itself the subject of an FTC investigation, Sheer stated that he was unaware of the relationship between Lifelock and Tiversa before being informed of it by Committee staff in a transcribed interview.

> Q. Are you aware of Tiversa and LifeLock having a -- having a business relationship -- I guess, what is your awareness of Tiversa and LifeLock's business relationship?
>
> A. I don't know that they have a business relationship other than the statement that was made in the -- in the email that you -- that you presented earlier.
>
> Q. Okay. Was the email I presented earlier the first you'd heard of Tiversa and LifeLock having any relationship?
>
> A. Yes.[219]

Boback could not have known the details of the FTC's investigations—including the timing of the letters, which constituted pre-decisional information about pending non-public government actions —without some sort of inside knowledge about the FTC's enforcement plans. While the Committee's investigation has not yet identified the source of the Tiversa's information about the FTC actions, it is clear that Tiversa and the FTC had a mutually beneficial relationship. The FTC used Tiversa as the source of convenient information used to initiate enforcement actions, and Tiversa used the FTC to in further pursuing the company's coercive business practices.

E. Information provided by Tiversa formed the basis of the FTC's case against LabMD

Documents produced to the Committee show that in an effort to generate business, Tiversa repeatedly sought to coerce companies to purchase its services. Tiversa's methods have ranged from contacting a company about a leak but failing to provide anywhere close to full information, to referring nearly 100 companies to the FTC. The Committee has spoken to numerous companies on the list Tiversa provided to the FTC—not one of the companies the Committee contacted had entered into a contract with Tiversa. One such business tangled in Tiversa's web was LabMD.[220] In January 2014, it closed its laboratory operations because of costs incurred by its dealings with Tiversa and the FTC.[221]

---

[218] *Id.* at 107.
[219] *Id*. at 170.
[220] *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight Gov't Reform*, 113th Cong., at 18 (July 24, 2014) [hereinafter Daugherty Testimony] (statement of Michael Daugherty, CEO of LabMD).
[221] *Id.* at 72.

According to Boback, Tiversa downloaded a file containing patients' personally identifiable health information in February 2008.[222] Tiversa determined that the downloaded file likely belonged to LabMD, and contacted the company in May 2008. Tiversa provided LabMD with a copy of the file, but would not provide the IP address or other information unless LabMD agreed to purchase Tiversa's services.[223]

Tiversa referred LabMD to the FTC as one of the companies listed in the spreadsheet as responsive to the FTC's CID. The FTC, in turn, sent a complaint letter to LabMD. The FTC then initiated an administrative enforcement action against LabMD for unfair and deceptive business practices.

Among the information Tiversa gave to the FTC regarding LabMD was the IP address that was the source of the leak. The origin of the IP address from where the LabMD document was pulled was a matter of contention in the litigation between LabMD and Tiversa. On numerous occasions, Boback maintained that Tiversa had pulled the LabMD document from an IP address in San Diego, California:

> Q. Going back to CX 21. Is this the initial disclosure source?
>
> A. If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.
>
> Q. When did Tiversa download CX 10?
>
> A. I believe it was in February of 2008.
>
> Q. Has CX 10 changed in any way since Tiversa downloaded it?
>
> A. No.[224]

When asked about the Georgia IP address, Boback denied downloading the information from there:

> Q. There is an IP address on the right-hand side, it is 64.190.82.42. What is that?
>
> A. That, if I recall, is an IP address that resolves in Atlanta, Georgia.
>
> * * *

[222] Fed. Trade Comm'n, Deposition of Robert Boback, In the Matter of LabMD, Inc. 25-26 (Nov. 21, 2013) [hereinafter Boback FTC Deposition].
[223] Daugherty Testimony, at 19.
[224] Boback FTC Deposition, at 25-26.

Q. What other information do you have about 64.190.82.42?

A. I have no other information. I never downloaded the file from them. They only responded to the hash match.[225]

In an internal e-mail dated almost three months before the deposition and never produced to the FTC, however, Boback stated that Tiversa downloaded the LabMD file while working for a client. He stated, "The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. This statement, made by Boback in September 2013, fundamentally calls into question his claim that Tiversa never downloaded the LabMD file from the IP address in Georgia.[226]

From: Robert Boback <rboback@tiversa.com>
Sent: Thursday, September 5, 2013 3:20 PM
To: Dan Kopchak <dkopchak@tiversa.com>; Molly Trunzo <mtrunzo@tiversa.com>
Subject: Tiversa

I wanted to provide updated information regarding the question of litigation involving Tiversa. During our call, I discussed litigation in which Tiversa is a pla against our former patent firm. That is still ongoing. Earlier in 2013, Tiversa was also engaged in a separate litigation with a company called LabMD, which is base in Georgia. Tiversa, Dartmouth College and Professor Eric Johnson (Tuck Business School) was sued by LabMD by its CEO, Michael Daugherty as he alleged that Tiversa "hacked" his company in an effort to get a file containing nearly 9,000 patient's SSNs and medical information and provided the information to Dartmouth and Eric Johnson for a DHS-funded research project. Mr. Daugherty has little to no understanding of P2P or Information security which is what caused him to think that he was "hacked" and which resulted in his widespread government conspiracy theory that followed. He also suggested in the litigation that because he woul not do business with Tiversa to remediate the problem, that Tiversa "kicked the file over to the feds [FTC]" (and Dartmouth) and the FTC sent him a questionnaire about the breach, which caused him "great harm" due to the widespread "government shakedown of small business." He claimed that Tiversa was attempting to extort money from him to "answer his questions" as a part of the larger conspiracy. The reason that I did not mention this during our discussion is that the case was dismissed due to jurisdiction (his real estate attorney friend filed it in Georgia). He subsequently appealed two times, and lost both, the final of which was ruled on in February 2013. As an interesting sidebar to this story, Mr. Daugherty began writing a book about the government overreach and his great conspiracy theory o the government war on small business. When our attorneys learned of what was coming in the book (from his blog postings about the book), we quickly served his counsel with a C&D as his "true story" was full of inaccurate statements about me and Tiversa. Unfortunately, Mr. Daugherty sees himself as "Batman" (no joke) and he chose to continue on with his book and starting scheduling speaking engagements where he would discuss his "true story" about how the government is out to "get" small business and that the FTC and Tiversa (and presumably Dartmouth) are the ring leaders. His book, "Devil inside the Beltway" is to be released later this month. While I do not expect this book to be on the NY Times best seller list, I cannot sit idly by and allow such a gross distortion of the facts and mischaracterization of Tiversa, and me, in his efforts to sell his book and create a "name" for himself on any speaking tour.

That said, Tiversa filed a complaint in federal court today citing a number of counts including but not limited to Defamation, Slander, Libel, and others against Mr. Daugherty and LabMD. Tiversa is not litigious and it was our hope that he would conduct himself appropriately after receiving the C&D in November of 2012. But again, he sees himself as Batman.

Here is the real series of events that occurred in this case:

Tiversa, as you know, downloads leaked information on behalf of clients, individual, corporate and/or federal. In the process of downloading information, we often get files that are not related to our clients but are nonetheless sensitive. We call this "dolphin in the tuna net"....for example, if we were looking for "Goldman Sachs" and our system finds a file with the term "Goldman" in it. The file may have the name "Henry Goldman" but our system just saw "Goldman" and downloaded it, in the event it related to Goldman Sachs. After the file would be downloaded, it would be reviewed by an Analyst which would determine that it was NOT related to Goldman Sachs, but it may or may not include SSNs or other sensitive information. This was the case with LabMD.

In 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name "LabMD" in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. At this point, we were not positive that the file belonged to LabMD, but it seemed probable. We could have chosen to do nothing at all and pretend that we never saw the file. That approach would leave both LabMD and the 9000 victims at very high risk (and growing) of fraud and identity theft. Needless to say, we contacted the company to inform them of the file with their company name on it. After providing the file with all of the information that we had, the Mr. Daugherty asked us for addition mation that we did not have. We told him that we could perform the services but it would take a few weeks and would cost about $15K. After hearing this, h send him the SOW for the services. 3 weeks after providing the SOW and not hearing anything in return, I reached out to Mr. Daugherty to see if he re: SOW) and he told me never to contact him again with no further explanation. We didn't.

"The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."

[225] Boback FTC Deposition, at 41-42.

[226] E-mail from Robert Boback to Dan Kopchak and Molly Trunzo (Sept. 5, 2013 3:20 p.m.) ("The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located.") [TIVERSA-OGR-0028866].

Further, the initial report that Tiversa provided to a client about the LabMD document stated that the company first "observed" the LabMD file in San Diego, California on August 5, 2008.[227] Tiversa could not have downloaded the LabMD file from an IP address in San Diego in February 2008 if it did not even observe the file at this IP address until August 2008.

In light of the information uncovered by the Committee's investigation, it appears the FTC was misled as to how Tiversa came to possess LabMD's file, which has been a material fact in the litigation of the enforcement action. Mr. Sheer testified that, contrary to information provided to the Committee, the FTC had never been told that the file was originally downloaded in Atlanta, Georgia.

> Q. Did anyone from Tiversa ever tell you that they first downloaded the file from Atlanta, Georgia, and not from San Diego, California?
>
> A That wasn't what the testimony was.
>
> Q Have you seen any documents during the course of your investigation indicating that Tiversa first downloaded the document from Atlanta, Georgia, and not from San Diego, as it testified to the FTC?
>
> A. Not that I am aware of.[228]

The discrepancies in the accounts of Tiversa's downloading of the LabMD file and the information provided to the FTC call into question the FTC's processes for relying on third-party sources and integrity of its actions against LabMD.

Finally, Tiversa recently performed another forensic analysis on the LabMD file after inexplicably telling the FTC that Tiversa had provided misinformation about the case.[229] This analysis stated that the LabMD file was disclosed by an IP address in Atlanta, Georgia between March 7, 2007, and February 25, 2008.[230] Yet, this information does not comport with the facts of the case. When Tiversa contacted LabMD on [DATE], LabMD performed an investigation and found that a billing manager's computer had LimeWire P2P software installed, and was sharing the LabMD file. Why did Tiversa's systems determine that the Georgia IP ceased to share the LabMD file in late February 2008, when LabMD's own investigation determined that the file was still being shared months later? Why wasn't this information captured by Tiversa's technology?

All of this information not only calls into question Tiversa's technological capabilities, but also Tiversa's claim that it never downloaded the LabMD file from a Georgia IP address – a

[227] Tiversa Forensic Investigative Report for Ticket #CIG00081 (Aug. 12, 2008) [TIVERSA-OGR-0017461-17465].
[228] Sheer Tr. at 151.
[229] Boback Tr., at 130.
[230] Tiversa Forensic Investigation Report – LABMD0001 (June 4, 2014) [TIVERSA-OGR-0017467-17482].

critical fact in the case against LabMD. As described above, Tiversa's Eagle Vision software purportedly downloads a document every time it hits on a search term. While the software will not download a document from the same IP address twice, it will download the same file from different IP addresses, which indicates the spread of the document. To the Committee's knowledge, Tiversa has not explained in this investigation or other legal proceedings why the software did not download the file from the Georgia IP address. Even assuming that Tiversa was unable to download a file due to technological problems (for example, because the peer-to-peer user signed off while Tiversa was downloading the file), then its software would make another attempt to download the file the next time it was available. Boback has testified that the LabMD file was available on the peer-to-peer network. Either the software does not download a relevant file each time it spreads to a new IP address, which fundamentally calls into question Tiversa's capabilities, or Tiversa did download the LabMD file from the Georgia IP address, a key point in the FTC proceeding.

There is little reason to doubt Boback's statements made to two Tiversa employees—the e-mail clearly shows Boback describing Tiversa's role in the FTC's LabMD enforcement action. Why Boback wrote this e-mail is unknown. It is possible he wanted to make sure he had his facts straight before he was deposed in the FTC matter. Further, Dan Kopchak, to whom Boback sent the e-mail, replied with a draft that made minor edits to the narrative but did not change or question the statement that the IP originated in Georgia.[231] Therefore, information the Committee obtained shows that Boback's testimony that source of the IP address came from San Diego is not true. Boback's conflicting statements have broad implications for the future of litigation between LabMD and Tiversa, and calls into question other information he has provided to the FTC.

In short, LabMD witnessed both Tiversa's manipulative business practices and Tiversa's close relationship with the FTC. Evidence produced to the Committee shows that the FTC notified Tiversa of its investigatory schedule, so that Tiversa knew when the Commission would issue complaint letters and act accordingly.

A whistleblower's account of the LabMD saga suggests that the patient data file was only found emanating from a LabMD computer in Atlanta, GA. The whistleblower demonstrated for the committee in tremendous detail how he found IP addresses associated with known identify thieves (also referred to as "information concentrators") and created documents later provided to the FTC showing that the file was in the possession of known-identity thieves when in fact there is no evidence to suggest it was downloaded by anyone other than Tiversa. The reason for forging the IP addresses, according to the whistleblower, was to assist the FTC in showing that P2P networks were responsible for data breaches that resulted in likely harm, not just the exposure of the information from the source computer which could have been easily remedied.

[231] E-mail from Dan Kopchak to Robert Boback (Sept. 5, 2013 4:01 p.m.) (revisions from the earlier draft included changes such as "was" to "were;" qualifying "understanding of P2P Information security" to "*may have* caused him to think that he was 'hacked' and which *apparently* has resulted in his widespread government conspiracy theory that followed;" the deletion of "Needless to say," etc.) [TIVERSA-OGR-0025706].

Ultimately, LabMD began to wind down operations in January 2014 as a result of the FTC enforcement action.[232]

F. Tiversa withheld documents from the FTC

The Committee has obtained documents and information indicating Tiversa failed to provide full and complete information about work it performed regarding the inadvertent leak of LabMD data on peer-to-peer computer networks. In fact, it appears that, in responding to an FTC subpoena issued on September 30, 2013, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

1. Despite a broad subpoena request, Tiversa provided only summary information to the FTC about its knowledge of the source and spread of the LabMD file.

Initially, Tiversa, through an entity known as the Privacy Institute, provided the FTC with information about peer-to-peer data leaks at nearly 100 companies, including LabMD.[233] Tiversa created the Privacy Institute for the specific purpose of providing information to the FTC. Despite Tiversa's claims that it is a trusted government partner, it did not want to disclose that it provided information to the FTC.[234]

After the FTC filed a complaint against LabMD, the agency served Tiversa with a subpoena for documents related to the matter. Among other categories of documents, the subpoena requested "all documents related to LabMD."[235] In a transcribed interview, Alain Sheer, an attorney with the FTC's Bureau of Consumer Protection, told the Committee that the FTC did not narrow the subpoena for Tiversa. Sheer stated:

> Q. This is the specifications requested of Tiversa. No. 4 requests all documents related to LabMD. Do you know if Tiversa produced all documents related to LabMD?
>
> A. I am not sure what your question is.
>
> Q. Let me ask it a different way. Was the subpoena narrowed in any way for Tiversa?

[232] Michael J. Daugherty, *FTC Actions Force LabMD to Wind Down Operations* (Jan. 28, 2014), http://michaeljdaugherty.com/2014/01/29/labmd-winds-operations/.
[233] Boback Tr. at 42.
[234] *See* Tiversa, Industry Outlook, Government/Law Enforcement, *available at* http://tiversa.com/explore/industry/gov (last visited Nov. 21, 2014); Boback Tr. at 42-43.
[235] Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC Subpoena].

A. Not that I am aware of.[236]

In total, Tiversa produced 8,669 pages of documents in response to the FTC's subpoena. Notably, the production contained five copies of the 1,718-page LabMD Insurance Aging file that Tiversa claimed to have found on peer-to-peer networks and only 79 pages of other materials, none of which materially substantiated Tiversa's claims about the discovery of the file.

The information Tiversa gave the FTC included the IP address from which Tiversa CEO Robert Boback has claimed the company first downloaded the LabMD file, as well as other IP addresses that Tiversa claims also downloaded the file. The origin of the IP address from which Tiversa first downloaded the LabMD file was in dispute in other litigation between LabMD and Tiversa. On numerous occasions, including before the FTC, Boback maintained that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. Boback stated:

Q. What is the significance of the IP address, which is 68.107.85.250?

A. That would be the IP address that we downloaded the file from, I believe.

Q. Going back to CX 21. Is this the initial disclosure source?

A. If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.

Q. When did Tiversa download [the LabMD file]?

A. I believe it was in February of 2008.[237]

Boback also testified that Tiversa performed an investigation into the LabMD file at the request of a client.[238] In the course of this investigation, Tiversa concluded that an IP address in Atlanta, Georgia, where LabMD was headquartered, was the initial disclosure source of the document. Boback stated:

Q. There is an IP address on the right-hand side, it is 64.190.82.42. What is that?

A. That, if I recall, is an IP address that resolves to Atlanta, Georgia.

Q. Is that the initial disclosure source?

A. We believe that it is the initial disclosure source, yes.

---

[236] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer at 147 (Oct. 9, 2014).
[237] In the matter of LabMD, Inc., Deposition of Robert J. Boback, CEO, Tiversa, transcript at 24-25 (Nov. 21, 2013) [hereinafter Boback Nov. 2013 FTC Tr.].
[238] Boback Nov. 2013 FTC Tr. at 72-73 ("In 2008, when working for another client, we were attempting to identify the original disclosure source of the file that we discovered from 1 the San Diego IP address.").

Q. And what is that based on?

A. The fact that the file, the 1,718 file, when we searched by hash back in that time for our client, we received a response back from 64.190.82.42 suggesting that they had the same file hash as the file that we searched for. We did not download the file from them.

* * *

Q. So, I think you are telling me that chronologically this was the first other location for that file in juxtaposition of when you found the file at 68.107.85.250?

A. We know that the file in early February, prior to this February 25 date, was downloaded from the 68.107.85.250. Upon a search to determine other locations of the file across the network, it appears that on 2/25/2008 we had a hash match search at 64.190.82.42, which resolved to Atlanta, which led us to believe that without further investigation, that this is most likely the initial disclosing source.

Q. What other information do you have about 64.190.82.42?

A. I have no other information. I never downloaded the file from them. They only responded to the hash match.[239]

Boback's testimony before the FTC in November 2013 made clear that Tiversa first downloaded the LabMD file from an IP address in San Diego, California, in February 2008, that it only identified LabMD as the disclosing source after performing an investigation requested by a client, and that it never downloaded the file from LabMD.

2. Tiversa withheld responsive documents from the FTC, despite the issuance of the September 2013 subpoena. These documents contradict the account Boback provided to the FTC.

On June 3, 2014, the Committee issued a subpoena to Tiversa requesting, among other information, "[a]ll documents and communications referring or relating to LabMD, Inc."[240] This request was very similar to the FTC's request for "all documents related to LabMD."[241] Despite nearly identical requests from the FTC and the Committee to Tiversa, Tiversa produced numerous documents to the Committee that it does not appear to have produced to the FTC. Information contained in the documents Tiversa apparently withheld contradicts documents and testimony Tiversa did provide to the FTC.

[239] Boback Nov. 2013 FTC Tr. at 41.
[240] H. Comm. on Oversight & Gov't Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014).
[241] Tiversa FTC Subpoena.

An internal Tiversa document entitled "Incident Record Form," dated April 18, 2008, appears to be the earliest reference to the LabMD file in Tiversa's production to the Committee.[242] This document states that on April 18, 2008, Tiversa detected a file "disclosed by what appears to be a potential provider of services for CIGNA."[243] The Incident Record described the document as a "single Portable Document Format (PDF) that contain[ed] sensitive data on over 8,300 patients," and explained that "[a]fter reviewing the IP address, resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source."[244] The name of the file was "insuranceaging_6.05.071.pdf," which is the same name as the file in question in the FTC proceeding. According to the Incident Record, the IP address disclosing the file was 64.190.82.42—later confirmed to be a LabMD IP address.[245] Upon learning about the file, CIGNA, a Tiversa client, "asked Tiversa to perform Forensic Investigation activities" on the insurance aging file to determine the extent of proliferation of the file over peer-to-peer networks.[246]

An August 2008 Forensic Investigation Report provided the analysis CIGNA requested. This report identified IP address 64.190.82.42—the Atlanta IP address—as proliferation point zero, and the "original source" of the Incident Record Form.[247] A spread analysis included in the August 2008 forensic report stated that the file had been "observed by Tiversa at additional IP addresses" but made clear that Tiversa had not downloaded the file from either additional source because of "network constraint and/or user behavior."[248] Thus, according to this report, Tiversa had only downloaded the LabMD file from one source in Atlanta, Georgia by August 2008. This contradicts Boback's testimony that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. If Tiversa had in fact downloaded the LabMD file from a San Diego IP address in February 2008, then that fact should be included in this 2008 forensic report. It is not.

One of the two additional IP addresses is located in San Diego, California. It is a different IP address, however, than the one from which Tiversa claims to have originally downloaded the file.[249] Further, Tiversa did not observe that this San Diego IP address possessed the LabMD file until August 5, 2008.[250] Thus, according to this report, Tiversa did not observe any San Diego IP address in possession of the LabMD file until August 2008. Again,

---

[242] Tiversa Incident Record Form, ID # CIG00081 (Apr. 18, 2008).
[243] *Id*.
[244] *Id*. (emphasis added).
[245] *Id*.
[246] Tiversa, Forensic Investigation Report for Ticket #CIG00081 (Aug. 12, 2008). This letter uses the phrase "forensic report" to describe this and a second report created by Tiversa about the LabMD file because that is the title used by Tiversa. It is not clear what, if any, forensic capabilities Tiversa possesses.
[247] *Id*.
[248] *Id*.
[249] The IP address reported on the August 2008 forensic report that resolves to San Diego, California is 68.8.250.203. Boback testified, however, that Tiversa first downloaded the LabMD file from IP address 68.107.85.250 on February 5, 2008. Tiversa concluded in the report that the second IP address on which it observed the file was "most likely an IP shift from the original disclosing source."
[250] *Id*.

the report stands in stark contrast to Boback's testimony that Tiversa first downloaded the LabMD file from a different San Diego IP address in February 2008.

In addition, both the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report stated that the LabMD file was "detected being disclosed" in April 2008. Neither report indicated that Tiversa first downloaded the file from the San Diego IP address—an IP address not listed on either report—on February 5, 2008. Boback's deposition testimony and a cursory four-line document marked as exhibit CX-19 seem to be the only evidence that Tiversa first downloaded the LabMD file from a San Diego IP address in February 2008.

These documents contradict the information Tiversa provided to the FTC about the source and spread of the LabMD file. If Tiversa had, in fact, downloaded the LabMD file from the San Diego IP address and not from the Georgia IP address, then these reports should indicate as such. Instead, the San Diego IP address is nowhere to be found, and the Georgia IP address appears as the initial disclosing source on both reports.

Tiversa also produced an e-mail indicating that it originally downloaded the LabMD file from Georgia – and not from San Diego as it has steadfastly maintained to the FTC and this Committee. On September 5, 2013, Boback e-mailed Dan Kopchak and Molly Trunzo, both Tiversa employees, with a detailed summary of Tiversa's involvement with LabMD. Why Boback drafted the e-mail is unclear. He wrote, "[i]n 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name 'LabMD' in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."[251]

As noted above, according to Alain Sheer, a senior FTC attorney assigned to the LabMD matter, the FTC did not narrow the September 2013 subpoena requiring Tiversa to produce, among other documents, "all documents related to LabMD."[252] Tiversa withheld these relevant documents about its discovery and early forensic analysis of the LabMD file from the FTC. These documents directly contradict testimony that Boback provided to the FTC, and call Tiversa's credibility into question. Boback has not adequately explained why his company withheld documents, and why his testimony is not consistent with reports Tiversa created at the time it discovered the LabMD file.

It is unlikely that the LabMD file analyzed in the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report is different from the so-called "1718 file" at issue in the FTC proceeding, particularly given Boback's testimony to the FTC about how Tiversa's

[251] E-mail from Robert Boback, CEO, Tiversa, to Dan Kopchak & Molly Trunzo (Sept. 5, 2013) (emphasis added) [TIVERSA-OGR-0028866-67].
[252] Tiversa FTC Subpoena.

system names files.[253] If, however, the earlier reports do refer to a different file, then Tiversa neglected to inform the FTC of a second, similarly sized leak of LabMD patient information.

3. Tiversa's June 2014 forensic report is the only report provided to this Committee that substantiates Boback's claims.

Tiversa produced to the Committee a forensic report on the LabMD file that it created in June 2014. Tiversa created this report and others related to testimony previously provided to the Committee after the investigation began. While outside the scope of the FTC's subpoena due to the date of the document, this is the only report supporting Tiversa's claim that it first downloaded the file from the San Diego IP address. This report contradicts information Tiversa provided to CIGNA in the April 2008 Incident Record Form and August 2008 Forensic Investigative Report—documents created much closer to when Tiversa purportedly discovered the LabMD document on a peer-to-peer network. The fact that Tiversa created the only forensic report substantiating its version of events after the Committee began its investigation raises serious questions.

This most recent report states that Tiversa's systems first detected the file on February 5, 2008 from a San Diego IP address (68.107.85.250) not included in either of the 2008 documents. According to the spread analysis, this San Diego IP shared the file from February 5, 2008 until September 20, 2011. Yet, despite allegedly being downloaded before both the April or August 2008 reports, neither 2008 document mentions that Tiversa downloaded this document.

The June 2014 report also states that the LabMD IP address (64.190.82.42) shared the file between March 7, 2007 and February 25, 2008. Thus, according to this report, by the time Tiversa submitted an Incident Record Form to CIGNA in April 2008, the LabMD IP address was no longer sharing the file. Furthermore, the report does not describe why Tiversa's system did not download the file from the Georgia IP address, even though the technology should have downloaded a file that hit on a search term, in this case "CIGNA," each time a different computer shared the document. The June 2014 report includes no reference to the other San Diego IP address discussed in the August 2008 forensic report as being in possession of the LabMD file.

4. Tiversa did not make a full and complete production of documents to this Committee. It is likely that Tiversa withheld additional documents from both this Committee and the FTC.

On October 14, 2014, Tiversa submitted a Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity.[254] Chief Administrative Law Judge D. Michael

[253] Boback Nov. 2013 FTC Tr. at 40-41 (describing that a file's "hash" or title identifies "exactly what that file is." The title of the LabMD document described in the April and August 2008 documents is the same as the title of the document in the FTC proceeding).

Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose."[255] Tiversa included two e-mails from 2012 as exhibits to the Notice of Information. According to Tiversa, these e-mails demonstrate that Wallace could not have fabricated the IP addresses in question in October 2013, because he previously included many of them in e-mails to himself and Boback a year prior.[256]

Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission in the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. In its Notice of Information, Tiversa did not explain how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information and do not explain what exactly Wallace conveyed to Boback in November 2012 or why he conveyed it.

If Boback did in fact receive this information in November 2012, his June 2013 deposition testimony is questionable. It is surprising that Tiversa would have supplied inaccurate information to the FTC when Boback himself apparently received different information just months prior. Tiversa should have located and produced these e-mails pursuant to the September 2013 subpoena, and it should have been available for Boback's June 2013 deposition.

Tiversa's failure to produce numerous relevant documents to the Commission demonstrates a lack of good faith in the manner in which the company has responded to subpoenas from both the FTC and the Committee. It also calls into question Tiversa's credibility as a source of information for the FTC. The fact remains that withheld documents contemporaneous with Tiversa's discovery of the LabMD file directly contradict the testimony and documents Tiversa did provide.

VI. *Tiversa's Involvement with House Ethics Committee Report Leak*

A. The *Washington Post* breaks the story

On October 29, 2009, the *Washington Post* reported that the U.S. House of Representatives Committee on Ethics was investigating the activities of "more than 30

[254] Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request For Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014), http://www.ftc.gov/system/files/documents/cases/572572.pdf [hereinafter Notice of Information].
[255] *LabMD Case: FTC gets green light to grant former Tiversa employee immunity in data security case*, PHIprivacy.net, Nov. 19, 2014, http://www.phiprivacy.net/labmd-case-ftc-gets-green-light-to-grant-former-tiversa-employee-immunity-in-data-security-case/.
[256] Notice of Information at 4.

lawmakers and several aides."[257] The *Post* based its reporting on a "confidential House ethics committee [*sic*] report" inadvertently disclosed on a peer-to-peer network.[258] "A source not connected to the congressional investigations" provided the document to the *Washington Post*.[259] The Ethics Committee stated that a junior staffer released the document after installing peer-to-peer software on a home computer.[260] The staffer was subsequently fired.[261]

The *Washington Post*'s story indicated that the leaked "Committee on Standards Weekly Summary Report" provided summaries of non-public ethics investigations of nineteen lawmakers and several staff members, as well as non-public investigations into fourteen additional lawmakers undertaken by the Office of Congressional Ethics.[262]

The same day that the *Washington Post* published its story, Chairwoman Zoe Lofgren made a brief statement about the leak on the House floor.[263] News of the leak prompted a review of the House's information systems to determine whether there had been any breach beyond the inadvertent leak of the Ethics Committee document on the peer-to-peer network.

Tiversa began providing written information about the leak to the House Ethics Committee in early November 2009, after the *Washington Post* broke the story. Documents produced by Tiversa, however, show that Boback was aware of the leak and its significance more than a week before the story was published. On October 20, 2009, a Tiversa analyst e-mailed Boback the name, resume, and Facebook profile picture of a House Ethics Committee staffer.[264] The subject line of the e-mail read, "US Rep Ethics Doc Leaker."[265] On October 26, 2009, four days before the *Washington Post* published its story, Boback wrote an e-mail to executives at LifeLock. He stated:[266]

---

[257] Ellen Nakashima & Paul Kane, *Dozens in Congress Under Ethics Inquiry*, WASH. POST (Oct. 30, 2009), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/10/29/AR2009102904597.html.
[258] *Id*.
[259] *Id*. In a subsequent *Washington Post* online question and answer forum, the Post further described that the Ethics Committee document was brought to its attention by "a source familiar with those kinds of [peer-to-peer] networks." Washington Post Q&A with Carol Leonning 1 (Oct. 30, 2009), *available at* http://www.washingtonpost.com/wp-dyn/content/liveonline/discuss/transcript_politics131.htm (last visited Sept. 4, 2014).
[260] Nakashima.
[261] *Id*.
[262] *Id*.
[263] Chairwoman Lofgren stated, "I regret to report that there was a cyberhacking incident of a confidential document of the committee. A number of Members have been contacted by The Washington Post, which is in possession of a document. We don't know with certainty whether it is an accurate document, but we thought it important to state the relevance of the material." Statement of Congresswoman Zoe Lofgren, Cong. Record, Announcement by the Chairwoman of the Comm. on Standards of Official Conduct (Oct. 29, 2009).
[264] E-mail from Rick Wallace, Analyst, Tiversa, to Robert Boback, CEO, Tiversa (Oct. 20, 2009 12:34 a.m.) [TIVERSA-OGR-0026603 - 26604].
[265] *Id*.
[266] E-mail from Robert Boback, CEO, Tiversa, to Mike Prusinski, Vice President, Pub. Affairs, LifeLock, Todd Davis, CEO, LifeLock, and Clarrisa Cerda, Counsel, LifeLock (Oct. 26, 2009 7:37 a.m.) [LLOCK-OGR-0002009].

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, October 26, 2009 7:37 AM
To: Mike Prusinski; Todd Davis; Clarissa Cerda
Subject: RE: 60 minutes

As soon as I get the OK from the FBI, we will be off an running. We h[illegible] huge rings that we are tracking right now but I can't discuss as they are open investi[illegible]. We hired a new guy that came from the Secret Service to help us address these cr[illegible].

Also, there was a breach in House Ethics via P2P that the Washington Post will be writing a story about this week or next. Should be interesting...

"…there was a breach in House Ethics via 2P2 that the Washington Post will be writing a story about this week or next…"

Boback did not explain to LifeLock how he had become aware of the breach, or of the upcoming, and then-unpublished, *Washington Post* story.

While it is suspicious that Boback knew of the *Washington Post* story days before its publication, this Committee's investigation did not examine whether Boback or Tiversa acted as the initial source in providing the Ethics Committee document to the *Washington Post*. Documents produced by Tiversa showed that Boback provided information about the leak to the *Washington Post* reporter. On October 30, 2009, at 4:49 p.m., a *Washington Post* reporter e-mailed Boback asking whether a certain statement, including a quote from Boback, was accurate:[267]

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 4:49 PM
To: Robert Boback <rboback@tiversa.com>
Subject: RE: this accurate?

A confidential House Ethics Committee file that disclosed the status of dozens of investigations of lawmakers on issues ranging from influence lobbying to defense peddling is still available on public file-sharing computer networks, according to a security firm that specializes in scouring such networks for clients.
The document, a committee report from late July, has been downloaded by a handful of users in Washington DC, Houston, New York, Los Angeles, Toronto and London, said Robert Boback, chief executive of Tiversa Inc., the firm that was able to confirm the document was still on the networks yesterday and has technology capable of allowing it to see what tens of millions of computer users are searching for or downloading in real time on these publicly accessible networks.
The file was disclosed inadvertently by a junior staffer on the ethics committee, who apparently had stored the file on a home computer that had on it popular "peer-to-peer" software used for downloading free music and movies through file-sharing networks, Congressional sources said. The staffer could not be reached for comment. Her father said her attorney had advised that she not speak about the case.
The peer-to-peer premise is simple, and potentially risky. Anyone who has the software makes contents of their computer available to anyone else with the software on their computer through a "peer to peer" exchange bypassing the Web, as long as they are on a file-sharing network at the same time.
The staffer, who was the Committee's Web administrator and developed electronic spreadsheets and documents, was fired earlier this week, the sources said.

.....

Tiversa did not produce to the Committee any response Boback may have written. This is the earliest document produced to this Committee indicating that the document had "spread," i.e., that other peer-to-peer users had downloaded it. The *Washington Post* does not appear to have used Boback's quote or the information about the spread of the document in stories about the leak.

[267] E-mail from Ellen Nakashima, Wash. Post, to Robert Boback, CEO, Tiversa (Oct. 30, 2009 4:49 p.m.) [TIVERSA-OGR-0026594].

The reporter then e-mailed Boback regarding the origin of the leak. The first sentence reiterated the known information about the leaker, and the second sentence outlined generally how peer-to-peer networks operate:

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 7:47 PM
To: Robert Boback <rboback@tiversa.com>
Subject: RE: this accurate?

In the breach, the report was disclosed inadvertently by a junior staffer on the ethics committee, who apparently had stored the file on a home computer that had so-called "peer-to-peer" software, congressional sources said. The popular software, which is easily available online, allows computer users to share music or other files. But it also allows anyone with the software on their computer to access documents of another user without permission, as long as the users are on a file-sharing network at the same time.

Ellen Nakashima
The Washington Post
202 334 4419 direct
202 286 0552 cell

http://projects.washingtonpost.com/staff/articles/ellen_nakashima/

Again, Tiversa did not produce any response from Boback. The e-mail does further illustrate, though, that the reporter sought advice from Boback, at the very least, during the drafting of an upcoming piece.

Several hours later, the same reporter e-mailed Boback a third time with additional information about the leak, including "the latest" on the response by House leaders:[268]

[268] E-mail from Ellen Nakashima to Robert Boback (Oct. 30, 2009 8:08 p.m.) [TIVERSA-OGR-0026592].

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 8:08 PM
To: Robert Boback <rboback@tiversa.com>
Subject: amended

File sharing networks are made up of hundreds of millions of users who periodically log on and off, with 25 million or so being active at any given moment. The typical user, when searching for files, will reach only a small portion of the users on the network--from 30 to 3,000 people, depending on the connection strength.
A search on the word "meeting" may result in anything from a PTA meeting to an Iraqi operations meeting involving sensitive military details.

Here's the latest :
House leaders on Friday called for an "immediate and comprehensive assessment" of congressional cybersecurity policies, a day after an embarrassing data breach that led to the disclosure of details of confidential ethics investigations.
Speaker Nancy Pelosi (D-Calif.) and Minority Leader John A. Boehner (R-Ohio) said they had asked the chief administrative officer of the House to report back to them on the policies and procedures for handling sensitive data as a result of the breach. The breach led to the inadvertent dislosure of a House Ethics Committee document that summarized the status of investigations into lawmakers' activities on subjects ranging from influence peddling to defense lobbying.
"We are working diligently to provide the highest level of data security for the House in order to ensure that the operations of House offices are secure from unauthorized access," Pelosi and Boehner said in a statement.
The breach angered lawmakers who were the subject of previously undisclosed investigations and raised questions about the security of other senstive documents.
Rep. Gary Miller (R-Calif.), who was named in the document as having his real estate dealings under investigation, said he was so upset about the breach that he complained Thursday evening about the matter to Rep. Zoe Lofgren (D-Calif.), chairman of the ethics committee, during a series of roll-call votes.
"This is ridiculous and amateurish," he said of the breach in the committee's files.
Even as the House leadership sought answers — and the Ethics Committee moved to review its own security policies — the newly disclosed document remained available on public file-sharing computer networks, according to security experts. As of Friday, it had been downloaded by users in Washington, New York, London and elsewhere.

Ellen Nakashima
The Washington Post
202 334 4419 direct
202 286 0552 cell

http://projects.washingtonpost.com/staff/articles/ellen+nakashima/

Again, Tiversa did not produce any response to this e-mail Boback may have written. It is therefore unclear if Boback did not respond at all to these three e-mails, responded by phone, or responded in e-mails that Tiversa failed to produce. In the third e-mail, however, information on the spread and availability is no longer attributed to Tiversa. Instead, it is attributed to "security experts." It is thus not clear if Boback asked that Tiversa not be named in the story, or if the reporter amended the information to exclude Tiversa's name without prompting. Two months later, in December 2009, Boback provided the same reporter with information about a TSA document Tiversa found on the peer-to-peer network. In that instance, Boback wrote, **"[a]s always, we are not the source. :-)[.]"**[269] The reporter responded, asking **"[w]hat again is the main reason you don't want to be identified as the source – to avoid charge [*sic*] that you're doing this for commercial gain? To preserve relationship with govt [*sic*] customers?"**[270]

[269] E-mail from Robert Boback to Ellen Nakashima (Dec. 17, 2009 2:12 p.m.) [TIVERSA-OGR-0008473].
[270] E-mail from Ellen Nakashima to Robert Boback (Jan. 4, 2010 10:36 a.m.) [TIVERSA-OGR-0008473]. Even this exchange runs contrary to statements Boback made to a potential client in July 2008. At that time, Boback wrote about another Washington Post reporter, "I know that the WashPost reporter is actively scouring the file sharing networks to find any information relevant to 'DC-area businesses…especially government contractors.' For clarity, we would never provide any information or files to any reporter whether you decided to work with our firm or not, however he will probably find them on his own if he continues to search." E-mail from Robert Boback, CEO, Tiversa, to [Redacted Name], President/CEO [Redacted Company] (July 17, 2008 2:55 p.m.) (Emphasis and ellipsis in original) [TIVERSA-OGR-0019195. Given that Boback did, in fact, provide information to a reporter on at least one occasion, it is not clear if Boback lied to this customer about Tiversa's relationship with the media, or if Boback changed his mind about this policy sometime later.

Tiversa did not produce any response to this e-mail from Boback. As such, his reasoning remains unknown.

Less than a year later, in August 2011, Tiversa entered into a contract with TSA for peer-to-peer monitoring and remediation services. The potential value of the contract over five years was $1,548,000 and the scope of the project included "help[ing] the TSA avoid negative publicity and exposure through P2P file sharing networks."[271] TSA did not exercise all option years on the contract. The Committee does not know how many years of the contract passed before TSA ended its contract with Tiversa.

Tiversa received a great deal of press attention in the wake of the House Ethics leak. *Network World* reported that Tiversa had "seen the file at multiple locations including London, Toronto, Washington, Los Angeles, Texas and New York."[272] The leak also sparked additional media interest around Tiversa's previously announced peer-to-peer discoveries.[273] In one instance, a blogger reported that Tiversa discovered the document.[274] Boback insisted that Tiversa deny "discover[y]" of the exposed report to a blogger; he maintained that Tiversa only "investigated" the breach after he was made aware of its occurrence.[275] As of September 12, 2014, the article remained unedited.[276]

Whether or not Tiversa "discovered" the leak, the documents show that although Tiversa was aware of the leak, the company failed to report the leak to the House Ethics Committee, long before the *Washington Post reported* about it.

B. Tiversa "assists" the House Ethics Committee in its investigation

While Tiversa was aware of the Ethics Committee leak more than a week before it became public, Tiversa does not appear to have contacted the Ethics Committee about the leak

[271] Contract HSTS03-11-C-CIO554 (Aug. 3, 2011) [TIV-0000101-135].
[272] Jaikumar Vijayan, *Leaked House Ethics Document Spreads on the Net via P2P*, NETWORK WORLD (Oct. 30, 2009), *available at* http://www.networkworld.com/article/2252989/securityeaked-house-ethics-document-spreads-on-the/security/leaked-house-ethics-document-spreads-on-the-net-via-p2p.html (originally published in *Computerworld*) (last visited Sept. 9, 2014).
[273] J. Nicholas Hoover, *Bill Would Ban P2P Use by Federal Employees*, INFORMATIONWEEK (Nov. 18, 2009), *available at* http://www.informationweek.com/regulations/bill-would-ban-p2p-use-by-federal-employees/d/d-id/1084955 (last visited Sept. 9, 2014) ("In October, Tiversa provided the House Oversight and Government Reform committee [*sic*] with evidence that secret military documents on P2P networks had been downloaded in China and Pakistan and that personally identifiable information on U.S. soldiers was widely available.").
[274] John Pescatore, *The Security Risks of Consumerization Hit Home for US Congress*, GARNER BLOG NETWORK (Nov. 2, 2009), http://blogs.gartner.com/john_pescatore/2009/11/02/the-security-risks-of-consumerization-hit-home-for-us-congress/ (last visited Sept. 12, 2014).
[275] E-mail from Robert Boback, CEO, Tiversa, to Scott Harrer, Brand Dir., Tiversa (Nov. 11, 2009 10:54 a.m.) (In response to an article by John Pescatore that read "I live in the Washington DC area and much Beltway buzz about the Washington Post article on Tiversa's discovery of a House ethics report only available on a peer to peer music stealing file sharing network," Boback said, "Tiversa did not discover the document…. we need to let Pescatore know about that. We only investigated the breach.") [TIVERSA-OGR-0026558].
[276] Pescatore..

prior to publication of the story by the *Washington Post*. Tiversa appears to have first spoken with the House Ethics Committee on or around November 2, 2009.

On November 2, 2009, Boback provided information about the leak to the House Ethics Committee. Specifically, Boback provided a list of IP addresses at which the House Ethics Committee document had allegedly been downloaded:[277]

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Monday, November 02, 2009 10:13 AM
To: Stoddard, Clifford
Subject: File Spread Analysis (Tiversa)
Importance: High
Sensitivity: Confidential

Mr. Stoddard,

Please see (below) the preliminary file spread analysis that Tiversa performed. Per our discussion, I have instructed our Security Ops Team to issue takedown notices for all of the cases listed. We will continue to monitor to verify that a) no other instances of spread arise and b) the takedown notices are effective in removing the file from the PCs and therefore the network. The IP address in red below is the original source of the leak.

216.45.59.122	UNITED STATES	CALIFORNIA	LOS ANGELES	OC3 NETWORKS & WEB SOLUTIONS LLC
70.240.108.51	UNITED STATES	TEXAS	HOUSTON	AT&T INTERNET SERVICES SWBELL.NET
69.119.255.103	UNITED STATES	NEW YORK	YONKERS	OPTIMUM ONLINE (CABLEVISION SYSTEMS)
72.225.253.212	UNITED STATES	NEW YORK	NEW YORK	ROAD RUNNER HOLDCO LLC
99.234.251.73	CANADA	ONTARIO	TORONTO	ROGERS CABLE INC.
81.76.50.206	UNITED KINGDOM	ENGLAND	LONDON	ENERGIS UK
69.255.116.72	UNITED STATES	DISTRICT OF COLUMBIA	WASHINGTON	COMCAST CABLE
98.218.86.107	UNITED STATES	VIRGINIA	ALEXANDRIA	COMCAST CABLE
76.111.69.89	UNITED STATES	VIRGINIA	ARLINGTON	COMCAST CABLE
68.48.69.117	UNITED STATES	DISTRICT OF COLUMBIA	WASHINGTON	COMCAST CABLE

If you have any questions, please email or call.

Best Regards,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Expert.
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

The locations of the IPs—including Washington, D.C., Houston, New York, Los Angeles, Toronto, and London—were the same as those included in the e-mails from the *Washington Post* reporter to Boback several days earlier. In a later e-mail that same day, Tiversa provided additional information about when it first located the Ethics Committee document:[278]

[277] E-mail from Robert Boback, CEO, Tiversa, to Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm. (Nov. 2, 2009 10:13 a.m.) [TIVERSA-OGR-0002413].
[278] E-mail from Robert Boback to Clifford Stoddard (Nov. 2, 2009 4:44 p.m.) [TIVERSA-OGR-0002412].

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

"As an answer to your question below, the search that resulted in us finding the original source file occurred in early August. It is my assumption that it was the same day in which the source of the leak saved it to her home PC. The file, although downloaded in early August, was not reviewed by anyone here at Tiversa until recently (2 weeks ago)."

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Monday, November 02, 2009 4:44 PM
To: Stoddard, Clifford
Subject: RE: File Spread Analysis (Tiversa)
Sensitivity: Confidential

Hi Cliff,

Our systems first acquired the file in early August using the term "report." As we provide services for ID theft pro through our partner LifeLock, we issue several general search terms for information related to consumer security such as r ial, meeting, password, login, medical, insurance, etc. The results of these, and our other client specific search terms, are wnloaded to our storage arrays. We have algorithms and individuals who then review the data via specific criteria (either specific co sumer names, SSNs, DOBs, etc. or specific client names like Goldman Sachs, Cigna, Capital One etc.) to determine if our clients information has been exposed. Our searches and downloads happen continuously and downloads have averaged in excess of 100,000 new files per day. As an answer to your question below, the search that resulted in us finding the original source file occured in early August. It is my assumption it was the same day in which the source of the leak saved it to her home PC. The file, although downloaded in early August, was not reviewed by anyone here at Tiversa until recently (2 weeks ago). I am not sure if I had spoken to Oversight about this specific file as we were discussing several files at that time. Our system can also download additional files (in an automated fashion) from the same source IP in an effort to provide our CFAs (Cyber Forensic Analysts) with additional insight as to the identity of the source of the disclosure. In this situation, our system downloaded two resumes from one of the IP addresses. It was due to the resume that we were able to arrive at a suspected original source.

Unfortunately, there is no way to tell exactly when the secondary IP addresses downloaded the file.

We will continue to monitor for the presence of the file on the network as others may have downloaded the file in addition to the IPs provided. Once detected, we will issue takedown notices with the corresponding ISPs.

Best Regards,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

Before Boback sent any e-mails to the House Ethics Committee on November 2, he e-mailed a LifeLock executive about the leak as an "FYI," in case LifeLock "want[ed] to piggyback anything on this[.]"[279]

[279] E-mail from Robert Boback, CEO, Tiversa, to Mike Prusinski, Vice President, Pub. Affairs, LifeLock (Nov. 2, 2009 9:50 a.m.) [LLOCK-OGR-0002036].

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, November 02, 2009 9:50 AM
To: Mike Prusinski
Subject: File sharing breach in House Ethics
Attachments: 20091029183511871.pdf

Pru,

Not sure if you saw the latest file sharing breach in Congress. See attached letter that Congress released regarding the breach. Congress is now doing a complete cybersecurity review and analysis. :-)

Just an FYI for you guys....not sure if you want to piggyback anything on this for your purposes....

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

"...not sure if you want to piggyback anything on this for your purposes..."

Several days later, Boback traveled to Washington, D.C. to meet with the Chair and Ranking Member of the House Ethics Committee regarding the leak.[280] During this meeting, the Ethics Committee appears to have requested a timeline from Tiversa about the leak.[281] On November 24, the Ethics Committee again requested a timeline, apparently after additional phone conversations between the Committee and Tiversa.[282] On December 3, the Ethics Committee requested yet again that Tiversa provide the timeline first requested nearly a month earlier. The Ethics Committee also asked if Tiversa's systems had picked up the file's download from Wikisecrets.org and several other websites:[283]

[280] E-mail from Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm., to Robert Boback, CEO, Tiversa (Nov. 6, 2009 2:30 p.m.) [TIVERSA-OGR-0002411].
[281] E-mail from Blake Chisam, Staff Dir. & Chief Counsel, Comm. on Standards of Official Conduct, to Robert Boback, CEO, Tiversa (Nov. 24, 2009 2:43 p.m.) ("I know Cliff's been chatting with you about the timeline that the Chair and Ranking Member discussed with you at our meeting … I can't recall seeing a timeline. Is there any chance you could shoot that over to me?") [TIVERSA-OGR-0002409]. Tiversa has not produced any documents to this Committee indicating that it replied to this request for information.
[282] *Id*.
[283] E-mail from Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm., to Robert Boback, CEO, Tiversa (Dec. 3, 2009 7:20 a.m.) [TIVERSA-OGR-0002407].

On Dec 3, 2009, at 7:20 AM, "Stoddard, Clifford" <Clifford.Stoddard@mail.house.gov> wrote:

Bob,

Sorry to pester you but in turn I am being asked continually about the time-line issue. I understand that Tiversa system discovered the document on August 4. The global search was done on October 30. Between then, you notified the Oversight Committee, specifically, Steven Rangel. Did you find out the specific date you notified Rangel? Also, as you probably know, the document has now been made available by Wikisecrets.org and can be downloaded from several websites. Did your system pick up these new addresses?

Also, could you have someone send us the hash for the file? Thanks.

The Members will be meeting with us in an hour and will ask again for the timeline I am sure.

Regards,

Cliff

Clifford C. Stoddard, Jr.

Counsel

Committee on Standards of Official Conduct

U. S. House of Representatives

HT-2, the Capitol

Washington DC 20515

(202) 226-8810 (direct)

Boback finally responded, with a very general timeline of events:[284]

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Thursday, December 03, 2009 10:32 AM
To: Stoddard, Clifford
Subject: Re: information

Hi Cliff
I am in LA training with FBI LEEDA right now but I wanted to drop you a note in advance of your meeting. Our systems located the file on Aug 1 not Aug 4. We did perform a global scan on Oct 30. I spoke to Steven Rangel between those dates but I don't have any record of it to provide clarity as to when. During that period I probably had 15 or so conversations with him regarding other breaches. To the best of my recollection, I think that I spoke to him about the document around the week of 19th of Oct, altough it may have been sooner. We only discussed it once. Beyond that, I don't specifically recall anything. It didn't seem that sensitive to me.

Best
Bob

Sent from my iPhone

Boback did not address the Ethics Committee's concern that the file had been made available by wikisecrets.org and several other websites. Boback also provided information that contradicted his November 2, 2009, e-mail. On November 2, Boback wrote that he "was not sure if [he] had spoken to Oversight about this specific file as we were discussing several files at that time."[285] On December 3, 2009, however, Boback wrote that he spoke with an Oversight Committee staffer sometime between August 1 and October 30, likely around October 19.[286]

[284] E-mail from Robert Boback to Clifford Stoddard (Dec. 3, 2009 10:32 a.m.) [hereinafter Boback-Stoddard Dec. 3 E-mail] [TIVERSA-OGR-0002407].
[285] E-mail from Robert Boback to Clifford Stoddard (Nov. 2, 2009 4:44 p.m.) [TIVERSA-OGR-0002412].
[286] Boback-Stoddard Dec. 3 E-mail..

Boback further explained that he "probably had 15 or so conversations" with the Oversight staffer about other breaches between August 1 and October 30, and that he only discussed the Ethics file with the Oversight staffer on one occasion. Boback explained that the file "didn't seem that sensitive" to him.[287]

Further, Boback indicated in the November 2 e-mail that Tiversa reviewed the House Ethics document "about two weeks ago," meaning that Tiversa became aware of the House Ethics file in mid-October. This timeline fits with an October 19 conversation with the Oversight staffer, and the October 20 internal Tiversa e-mail in which Boback received information about a House Ethics staffer.

Tiversa, by its own admission, learned of the House Ethics document in mid-October. Boback had a conversation about the document with the House Oversight Committee, mentioned the leak to executives at LifeLock, and conducted an investigation into the source of the leak, all before publication of the story. Yet Tiversa does not appear to have contacted the House Ethics Committee about the leak prior to publication of the *Washington Post* story. Boback further appears to have provided information about the spread of the leak to the *Washington Post* days before he provided the same information to the Ethics Committee.

Had Tiversa notified the Ethics Committee about the leak in a timely fashion, then it could have prevented some or all of the alleged spread of the document over the peer-to-peer network. When presented with a chance to minimize harm to the House of Representatives, Boback failed to act. Instead, Boback's failure to inform the House Ethics Committee of the leak quickly and his failure to provide timely and consistent information about the exposed document are indicative of Tiversa's questionable business practices in general. Finally, Tiversa stood to benefit from the *Washington Post*'s publication of the House Ethics leak regardless of whether Tiversa was the initial source of the article, or whether the article cited Tiversa. Any news on the vulnerability of sensitive information to leaks breached via peer-to-peer networks—and especially a high-profile breach—would bolster Tiversa's profile as a firm with the capability to remediate this type of problem. The House Ethics leak is another example of Tiversa's use of its association with Congress as a platform for intimidation and fearmongering.

A whistleblower's account of the story states that in the course browsing the P2P network for profitable material, Tiversa came across the Ethics Committee document. Tiversa's plan, according to the whistleblower was to leak the document to the press and generate publicity for it and then sell its services to the U.S. congress as the solution to the problem while never acknowledging it was the source of the breach. This resulted needlessly in the embarrassment of many Members of Congress who did not receive investigatory due process as a result of the pending investigations being exposed.

VII. *Open Door Clinic*

[287] *Id*.

The Open Door Clinic is a small non-profit healthcare organization located in Elgin, Illinois.[288] Open Door provides education, testing, and treatment for sexually transmitted infections, including HIV/AIDS.[289] Between 2008 and 2009, Tiversa sought to exploit the Open Door Clinic using information Tiversa discovered on a peer-to-peer network.

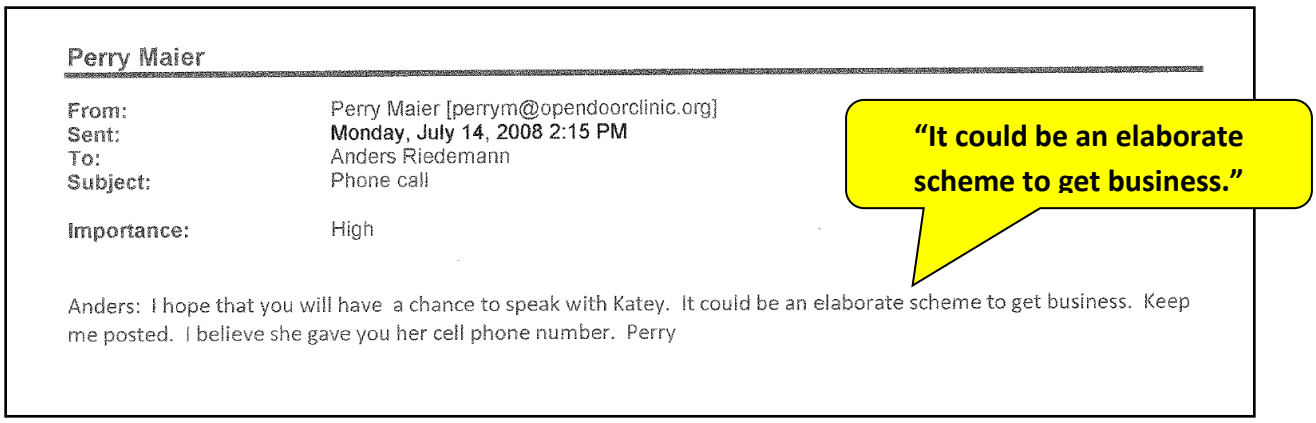
A. Initial contact with Tiversa

On June 5, 2008, a computer with the IP address of 75.58.87.97 disclosed six files related to the Open Door Clinic on a peer-to-peer network.[290] According to information provided by Tiversa, through the Privacy Institute, to the FTC, Tiversa appears to have downloaded these six files from that IP address on or around June 5, 2008.[291] The documents—spreadsheets of patient information—exposed the names, addresses, telephone numbers, social security numbers, and HIV/AIDS status of approximately 250 Open Door patients.[292] The fact that patient information was leaked on a peer-to-peer network is not disputed, nor is the seriousness of the leak in question. The documents contain no information identifying them as the property of the Open Door Clinic— the clinic's name does not appear on any or the six spreadsheets, nor does its address, phone number, location, or any identifying information appear.[293] Tiversa has not provided information to the Committee about how it determined that these documents belonged to the Open Door Clinic.

On July 14, 2008, a Tiversa sales representative contacted the Open Door Clinic about the leak.[294] Tiversa subsequently provided one of the six documents it downloaded to the Open Door Clinic via e-mail.[295] In the e-mail, which included the password to open the document, the

[288] *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 113th Cong. 25 (July 24, 2014) (testimony of David Roesler, Exec. Dir. of Open Door Clinic) [hereinafter Roesler Testimony].
[289] Open Door Clinic, *History*, *available at* http://www.opendoorclinic.org/about-us/history/ (last visited Sept. 4, 2014).
[290] Microsoft Excel spreadsheet from Tiversa to FTC, "FTC Final 8-14-09pm.xls" [FTC_PROD0000014].
[291] *Id*. The exact date of download of all six documents is not fully clear to the Committee. The spreadsheet of companies created by Tiversa for the FTC indicates that the "date of disclosure" of the six Open Door Clinic files was June 5, 2008. *Id*. Tiversa informed the Committee, however, that it downloaded one of the files, "Master List.xls," on May 26, 2008 at 7:29 p.m. Letter from Reginald J. Brown, Counsel for Tiversa, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2014). Tiversa declined to provide the exact dates it downloaded the additional five files related to the Open Door Clinic "because Tiversa, Inc. believes it only analyzed the origins of the MASTER LIST.xls file." *Id*. It is not clear how Tiversa determined the date of disclosure of the six files provided to the FTC to be June 5, 2008, and why Tiversa did not inform the FTC that at least one of the files provided was downloaded the previous month. It is also not clear how Tiversa provided a "date of disclosure" to the FTC for all six documents if it in fact only analyzed one of the files.
[292] Microsoft Excel spreadsheet from Tiversa to FTC, "Master List.xls" [FTC_PROD0005345].
[293] Microsoft Excel spreadsheets from Tiversa to FTC, "Master List January 15, 2003.xls" [FTC_PROD0005340]; "Master List Michelle.xls" [FTC_PROD0005341]; "Master List Rosa.xls" [FTC_PROD0005342]; "Master List Sally.xls" [FTC_PROD0005343]; "Master List Sharon.xls" [FTC_PROD0005344]; "Master List.xls" [FTC_PROD0005345].
[294] E-mail from Perry Maier, Assistant Dir., Open Door, to Anders Riedemann, IT Adm'r, Adnet (July 14, 2008 10:56 a.m.).
[295] E-mail from Keith Tagliaferri, Cyber Forensic Analyst, Tiversa, to Anders Riedemann, IT Adm'r, Adnet (July 14, 2008 3:20 p.m.).

sales representative attached a statement of work for the Open Door Clinic to hire Tiversa.[296] The quoted rate for Tiversa's services was $475 per hour – far beyond the clinic's modest budget.[297] Open Door employees were immediately suspicious as to why Tiversa contacted the clinic:[298]



The Open Door Clinic began an internal investigation of the leak after receiving notification from Tiversa. In early September 2008, an IT vendor for the clinic contacted Tiversa by telephone to obtain more information about the leak and what steps the clinic could take to remediate the breach.[299] Tiversa provided eight steps that Open Door could undertake to remediate the leak:[300]

[296] E-mail from Katy Everett to Anders Riedemann, IT Adm'r, Adnet (July 14, 2008 3:29 p.m.) [Open Door e-mail #5].
[297] Roesler Testimony, at 25.
[298] E-mail from Perry Maier to Anders Riedemann (July 14, 2008 2:15 p.m.).
[299] E-mail from Katy Everett, Tiversa, to TJ Vinz, Adnet (Sept. 4, 2008 1:34 p.m.).
[300] *Id*.

Tuesday, January 26, 2010 1:26 PM

bject: P2P Disclosure Information
ate: Thursday, September 4, 2008 1:34 PM
From: Katy Everett <keverett@tiversa.com>
To: TJ Vinz <tvinz@adnet.us>

Hi TJ. Thank you for taking the time to speak with me on the phone this afternoon. What follows is some information you can share with the folks at Open Door in terms of recommendations we would make or best practices we have seen others follow when facing similar circumstances regarding a potential breach. First, please know that though this type of incident is not a new problem, the exposure of it as an issue is new. Extremely large companies with very sophisticated IT systems have been victim to sensitive and costly P2P disclosures (such as Pfizer, ABN AMRO, Walter Reed Army Medical Hospital, etc.) and few if any organizations are immune to its risk.

When a disclosure like this occurs, companies often go through the following steps:

1. Identify the offending computer/source (it may or may not be the computer that you have identified)
2. Identify any additional files that might have been disclosed from the offending computer/ source (this often determines/confirms the original source because often additional files are disclosed that allow us to profile the individual disclosing them)
3. Remediate/close down the offending computer/source
4. Identify any additional sources that may have acquired the file(s) and are re-sharing it/ them to the P2P networks
5. Remediate/close down any additional sources found in step #4
6. Take any notification steps required by state/industry regulatory bodies based on the severity of the information disclosed (e.g. social security numbers, etc.)
7. Provide services (e.g. credit monitoring, fraud alerts, etc.) to affected individuals
8. Document all steps taken to address both this incident and to prevent others from occurring as required by state/regulatory bodies, customers, other stakeholders, etc., and in support of any future legal defense actions

As I said earlier, Tiversa can assist Open Door with any of the above and in performing the global spread analysis we discussed. This helps many organizations inform their security breach notification proceedings as it will tell you how far the file has spread and how many pcs currently have downloaded it. As we discussed, even though the file itself may appear old, social security numbers never expire and criminals hunt for them every day on these networks in an effort to commit identity theft or fraud against individuals.

Tiversa also offered to "assist Open Door with any of the above and in performing the global spread analysis we discussed."[301] The sales representative again attached a statement of work for an Incident Response Investigation for Open Door. The quoted rate remained $475 per hour.[302]

One hour later, the Open Door Clinic's IT vendor sent these eight steps to the clinic, as well as information on how the clinic had already addressed each step in the course of its internal investigation.[303] The clinic's internal investigation, based on the limited information provided by

[301] *Id*.
[302] *Id*.
[303] E-mail from TJ Vinz, Adnet to Ryan Howater, Adnet (Sept. 4, 2008 2:40 p.m.).

Tiversa, found that none of the computers on the system had peer-to-peer software installed, and that no peer-to-peer network ports into or out of the clinic's computer system were allowed.[304] As Executive Director David Roesler testified, the clinic was at a loss as to how the one file Tiversa provided could have been exposed on a peer-to-peer network.[305]

Later that month, Tiversa again contacted the Open Door Clinic, this time attempting to sell LifeLock's identity theft services.[306] A Tiversa sales representative wrote, "Tiversa has recently established an exciting new partnership with a company called LifeLock. LifeLock is a leading provider of identity theft PREVENTION [*sic*] services to many organizations and corporations."[307]

Ultimately, Open Door declined to purchase Tiversa and LifeLock's services. In his testimony before the Committee, Roesler explained that the clinic did not purchase Tiversa's services because Open Door's IT provider had sufficiently "reviewed its network to confirm that there was no evidence of any P2P software."[308]

B. Tiversa only provided self-serving information to the Open Door Clinic in July 2008

Tiversa has maintained to the Committee that it went above and beyond in trying to help the Open Door Clinic mitigate the peer-to-peer leak. Such a statement, however, is not only self-serving, but also incorrect. In fact, Tiversa failed to provide full and complete information about the leak to the clinic.

Several of the eight steps for mitigation Tiversa suggested to the clinic—including the suggestions to "identify any additional sources that may have acquired the file(s) and are re-sharing them to the P2P networks" and "remediate/close down any additional sources found in step #4"—are steps that seemingly require the use of Tiversa's technology. Tiversa has maintained that it provides technology and services that no other company can provide. The so-called "steps" Tiversa provided are in fact a blatant sales pitch. Tiversa failed to provide additional files downloaded from the Open Door Clinic on the same day from the same IP address. Tiversa also failed to provide the IP address of the computer leaking the files, information that Tiversa's technology can provide in minutes. Had Tiversa chosen to provide the Open Door Clinic with this information, the clinic could have more readily identified the source of the leak.

Further, Tiversa appears to have begun investigating the source of the Open Door leak even prior to July 14, 2008, when it first contacted the Open Door Clinic. On July 3, 2008, Chris

[304] *Id*.
[305] Roesler Testimony, at 25.
[306] E-mail from Katy Everett, Tiversa, to TJ Vinz, Adnet (Sept. 24, 2008 2:20 p.m.). This e-mail was not produced to the Committee by Tiversa.
[307] *Id.*
[308] Roesler Testimony, at 25, 60.

Gormley, Tiversa's former Chief Operations Officer, e-mailed a sales representative a web link, with the notation "Open Door Clinic:"[309]

Molly Trunzo

From: Chris Gormley
Sent: Thursday, July 03, 2008 11:26 AM
To: Katy Everett
Cc: Chris Gormley
Subject: Info

http://www.effectiveinterventions.org/go/interventions/sista

Open Door Clinic

Tiversa did not produce this e-mail to the Committee. A forensic report Tiversa created in October 2011, which Tiversa also did not produce to the Committee, includes several files about the "SISTA Project" to support its conclusion that the probable disclosure source was a specific Open Door employee.[310]

The July 3, 2008, e-mail indicates that Tiversa had already begun work on step one of the eight steps provided to the Open Door Clinic—"identify the offending computer/source"—but failed to inform Open Door of this information. Further, the same sales representative who sent the eight steps to the Open Door Clinic also received Gormley's e-mail.

Had Tiversa really wanted to help this non-profit clinic, it could have provided all of the files downloaded from Open Door and the IP address of the computer sharing the files in question. Tiversa could have also informed the clinic that it had already begun investigating the source of the breach, and had identified a potential link between documents the computer shared and the identity of the computer's owner.

C. Tiversa facilitates a class action lawsuit against the Open Door Clinic, and contacts Open Door patients directly

On July 29, 2009, Tiversa CEO Robert Boback testified about the Open Door Clinic leak before the Committee. Boback stated that 184 Open Door patients were "now victims of identity

[309] E-mail from Chris Gormley, COO, Tiversa, to Katy Everett, Tiversa (July 3, 2008, 11:26 a.m.) [hereinafter July 3 Tiversa E-mail].

[310] Tiversa, *Forensic Investigation Report: Open Door Clinic*, at 6, 21, 26, 29 (Oct. 13, 2011). One of the excerpted documents in the Investigative Report discusses the SISTA Training Institute, and refers participants to the website www.effectiveinterventions.org – the same main website as the link in Gormley's July 3, 2008 e-mail (July 3 Tiversa E-mail).

theft."[311] After this hearing, a Committee staffer expressed concern to Boback that the affected Open Door clients had not been notified that their personal information had been exposed.[312]

Rather than contacting the Open Door Clinic to provide additional information about the leak that Tiversa initially withheld, such as the IP address of the source computer, the additional files that Tiversa downloaded, or any investigation Tiversa performed into the identity of the disclosing source, Boback provided information on the Open Door leak to Michael Bruzzese, one of Tiversa's attorneys.[313] Shortly after the July 2009 hearing, Boback provided Bruzzese with a verbal summary of what he knew about the Open Door leak.[314] Boback also provided one of the six documents Tiversa downloaded from the clinic.[315] At this time, Boback stated that Tiversa had also determined that an "information aggregator" located in Apache Junction, Arizona downloaded Open Door's documents.[316] Boback did not provide Bruzzese with information about any other spread at this time.[317] Boback also did not provide the Open Door Clinic with information about the alleged spread of the file.

Bruzzese and his co-counsel "retained the services of an attorney who devotes his practice to matters involving legal ethics and the rules of professional responsibility to provide us legal advice as to how and in what manner we could solicit potential clients for this case."[318] Bruzzese determined that "it was permitted to contact the potential class members by mail" and sent letters to all patients on the list Boback provided.[319] The letter was a "solicitation to provide legal services," and asked the recipient to sign on as a class representative for the suit.[320]

Tiversa, through one of its current attorneys, explained to the Committee why Tiversa provided information to Bruzzese instead of contacting Open Door or its patients directly. The attorney stated that Tiversa did not have the resources to contact the patients itself, and accordingly provided the information to an attorney:

---

[311] *Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. 12 (July 29, 2009) (testimony of Robert Boback, CEO of Tiversa, Inc.). Michael Bruzzese, however, told the Committee that he did not know what would have been the basis of this statement; he was not aware of any claims of identity theft until after he assembled plaintiffs for the class action lawsuit between November 2009 and February 2010. H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Michael Bruzzese, at 115 (Sept. 10, 2014) [hereinafter Bruzzese Tr.].

[312] Letter from Michael J. Bruzzese, Att'y, Johnson, Bruzzese & Temple, LLC, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform 2 (July 30, 2014) [hereinafter July 30 Bruzzese Letter].

[313] *Id.*

[314] Bruzzese Tr. at 21-22.

[315] *Id.* at 22.

[316] *Id.* at 32. A draft version of the Tiversa Forensic Investigation Report includes a file spread analysis. This analysis indicates that the file spread to four IP addresses unrelated to the initial disclosing source. The spread analysis shows that, in addition to the Apache Junction user, a peer-to-peer user in the Netherlands had also downloaded at least one of the Open Door files on March 12, 2009. It is not clear how Boback knew about the spread of the file in one instance, but not the other. Tiversa, *Forensic Investigation Report: Open Door Clinic* (Oct. 21, 2011) (draft report). At no point was Tiversa's file spread analysis provided to the Open Door Clinic.

[317] Bruzzese Tr. at 32-33.

[318] July 30 Bruzzese Letter at 2.

[319] *Id.*; *see also* Letter from Michael Bruzzese & James Cirilano, Cirilano & Associates, to [Open Door Clinic Patient] (Nov. 4, 2009) [hereinafter Bruzzese Patient Letter].

[320] Bruzzese Patient Letter..

> Here's what our understanding is. And, again, I think you're going to get a letter. . . . Tiversa found the Open Door file. They called them, as is their policy, just saying, look, we found this on your system, here it is. They said, no, thanks, about getting help.
>
> Getting ready for the testimony in 2009, they told the story to someone on staff. And when they told them the story, they were told back that somebody needs to reach out to the victims.
>
> **Tiversa did not have the resources to do it themselves, and they just gave a file to the local Pittsburgh attorney**, who they knew, in order to help the victims. And Tiversa didn't get any payment for it.[321]

He further stated:

> Well, what he did with it, I don't think -- Tiversa didn't say, go do this or that. It was, they were asked by staff to make sure the victims knew that their information was compromised. **And since they didn't have the ability to do it themselves, or more than what they did, they gave the information to this guy, and he said he would handle it.**[322]

Bruzzese also explained to the Committee how he contacted the clients of the Open Door Clinic. He stated:

> Q. How did you contact [the Open Door clients]?
>
> A. We contacted them one way, the only way, by sending them what in our profession is called an attorney solicitation letter, and prior to doing that, I retained the services of a lawyer in Pittsburgh who kind of concentrates his area of practice on professional responsibility and ethics and asked him whether and how under Illinois law that I could contact these individuals. And he did some research, told me **that I was prohibited from making direct phone calls to them but that I could send a letter as long as I marked on the letter that it was a solicitation from a lawyer.** And that's what we did.
>
> * * *
>
> A. Correct. So let me just make a statement to you. **Prior to the five individuals retaining my services as their lawyer, I did not make any telephone calls to any Open Door Clinic patients.**

[321] Hopkins Tr.at 143-44.
[322] *Id*. at 145 (emphasis added).

Q. Did you ask Mr. Boback if Tiversa could make telephone calls to any of the Open Door patients?

A. No.

Q. **Did you ask Mr. Boback to contact the Open Door patients in any way?**

A. **No.** [323]

Documents obtained by the Committee, however, show that Tiversa independently contacted patients of the Open Door Clinic about the leak.[324]

As these documents call into question information provided by Tiversa to the Committee, the Committee obtained phone records showing long-distance calls from Tiversa's office during the time in question. **A comparison of the phone records to documents Tiversa downloaded from the Open Door Clinic, which contained patients' personal information, clearly shows that Tiversa called more than 50 patients of the Open Door Clinic between October 29 and November 5, 2009.** Tiversa called at least one patient on multiple occasions. These phone calls from Tiversa took place just days before Bruzzese sent a letter to Open Door patients.

It is not clear why Tiversa provided false information to the Committee about whether the company contacted any Open Door patients. Further, it is not clear why Tiversa lacked the resources to contact Open Door patients, as the company represented to the Committee through its attorney. In fact, Tiversa did contact over 50 patients of the clinic. It is also not clear why Tiversa would contact over 50 patients of the clinic in late October and early November 2009, days before Bruzzese sent a letter to patients of the clinic, and following the Committee staffer's July 2009 alleged notification that patients needed to be notified.

In September 2009, Tiversa again contacted Open Door to report that the breached document was still exposed on the peer-to-peer network.[325] Again, Open Door performed its own investigation of its servers and again found no evidence of any peer-to-peer networks.[326] Tiversa did not tell Open Door that it had referred information about the leak to an attorney, nor did Tiversa provide any of the information previously withheld from the clinic. Although Tiversa professed it was concerned about notifying the patients of Open Door about the leak of personally identifiable information, it still omitted key information.

Six patients agreed to join the class action against the Open Door Clinic, and Bruzzese filed the lawsuit in February 2010. During discovery, Open Door subpoenaed Tiversa and

[323] Bruzzese Tr. at 35-36 (emphasis added).
[324] *See, e.g.* e-mail from Barb Cox to David Roesler, Dir., Open Door Clinic (Nov. 5 2009 4:29 p.m.) ("According to [redacted]-triversa [*sic*] called him first and asked a ton of questions-did they know that open door had done this etc. I think that Triversa [*sic*] is affiliated with the law firm and sent them the info they had-I would imagine that they get a finders fee [*sic*].").
[325] Roesler Testimony, at 25.
[326] *Id.* at 25-26.

finally received the additional files that Tiversa downloaded from the same computer on the same day as the one file it previously provided.[327] This production included information indicating that an IP address in Apache Junction, Arizona, downloaded all six Open Door files.[328] Bruzzese testified to the Committee that he also did not receive a full accounting of all the Open Door files Tiversa downloaded until he received Tiversa's production.[329]

After receiving full information from Tiversa, the Open Door Clinic determined that the source of the breach was a computer stolen from the clinic in 2007.[330] Open Door believes that the peer-to-peer software that exposed its patients' personally identifiable information was installed on the computer after it was stolen, and therefore was not a breach of Open Door's network.[331]

D. Tiversa did not charge Bruzzese for the same information it refused to provide to the Open Door Clinic

Tiversa did not accept payment for any services provided as part of the litigation against the Open Door Clinic.[332] When Boback first told Bruzzese about the Open Door leak, Boback was "adamant"[333] that Tiversa would provide any required services free of charge:

> He said, Tiversa does not want anything. I do not want anything. I am doing this to—words to this effect—discharge my obligation put upon me by the staffer to do something about it. **And he said that, whatever you need, in terms of forensic work, you've got, no matter what.**[334]

Pursuant to this professed sense of moral obligation, Tiversa performed forensic analysis of the Open Door Leak. Tiversa examined the source of the leak, including details about the 27 times the IP address shifted, the identity of the leak, and the alleged spread of the leak. Tiversa produced a 42-page forensic investigation draft report,[335] and a 39-page final forensic investigation report[336] for Bruzzese's use in the litigation.

Boback directed that Tiversa expend time and effort to investigate the leak for Bruzzese at no charge. He provided the exact same services to Bruzzese for free that he withheld from the Open Door Clinic. Had Boback really felt a sense of moral obligation to the patients of the Open

---

[327] *Id.* at 94.
[328] The production included a spreadsheet titled "Open Door Clinic File Listing With Spread" and included a list of files for two IP addresses. One IP address is the disclosing source as identified by Tiversa, and the other IP address at the time resolved to Apache Junction, Arizona. Tiversa Production to Open Door Clinic (Jan. 21, 2011).
[329] Bruzzese Tr. at 34.
[330] Roesler Testimony, at 91.
[331] *Id*. at 93.
[332] Bruzzese Tr. at 65-66.
[333] *Id.* at 65.
[334] *Id.*
[335] Tiversa, *Forensic Investigation Report* (Oct. 13, 2011.
[336] Tiversa, *Forensic Investigation Report* (Oct. 21, 2011)..

Door Clinic, he could have provided these services to the Open Door Clinic. Once again, Tiversa was in a position to help and refused to do so.

According to a whistleblower, Tiversa engaged in numerous attempts to get the Open Door Clinic to pay for its services. When the clinic refused, Tiversa began calling the patients listed on the document it downloaded. Tiversa employees thought that by calling the patients and ginning up the leak, they could scare the clinic into hiring Tiversa. When this plan failed, Boback provided the information to his attorney, Michael Bruzzese, who filed a law suit against the non-profit clinic while TIversa performed work related to the exposure free of charge to Bruzzese. The clinic was never informed by Bruzzese that Bruzzese received the information from Tiversa.

E. Tiversa provided information on the Open Door Clinic to the FTC

In addition to providing information to assist Bruzzese in his class action lawsuit, Tiversa also provided information on the Open Door Clinic leak to the FTC. Tiversa, through the Privacy Institute, provided all six documents about the clinic to the FTC. As noted above, the spreadsheet Tiversa provided indicated that all six documents were downloaded from the same IP address and disclosed on the same day – June 5, 2008.[337] On January 19, 2010, the FTC sent a letter to Open Door Clinic about the leak.[338] The letter informed the clinic that a file had been exposed on the peer-to-peer network, and noted that the clinic's failure to prevent the document from leaking could violate federal laws.[339]

If Boback was truly motivated to help the patients affected by the Open Door leak, he should have given complete information to Open Door immediately. Instead, Boback withheld critical information about the number of downloaded documents, the IP address of the leak, and any information Tiversa had uncovered about the source of the leak. He referred the leak to an attorney. Even after the referral, Tiversa made unsolicited calls to more than 50 patients of the clinic about the leak for unknown reasons. And, finally, Boback provided the very information and services he denied to the Open Door Clinic for free to the attorney who sued the Open Door Clinic over the leak Tiversa first identified. Boback's actions toward the Open Door Clinic unfortunately fit a pattern of self-promotion and manipulation, not a heartfelt wish to "discharge [his] obligation" to Open Door's clients.

VII. *Conclusion*

The Committee's investigation raises substantial questions about Tiversa's business practices. The company's failure to produce documents responsive to the subpoena hindered the Committee's investigation. Not only did Tiversa primarily report companies to the FTC that had

[337] Microsoft Excel spreadsheet from Tiversa to FTC, "FTC Final 8-14-09pm.xls" [FTC_PROD0000014].
[338] Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Protection, Federal Trade Comm'n, to Open Door Clinic (Jan. 19, 2014).
[339] *Id*.

refused its services, but it also manipulated its relationship with the FTC—including its knowledge of upcoming investigations—in an attempt to profit from these same companies the second time around. In addition, Tiversa seemingly knew about a breach at the House Ethics Committee nine days before the *Washington Post* reported about the breach. Boback notified LifeLock about the breach and the upcoming article, but failed to notify the House Ethics Committee itself. Boback's communications prior to the publication of the article call into question his claim that he did not act as the *Washington Post's* source. Finally, Boback's actions toward the Open Door Clinic are unethical, and potentially illegal. Boback refused to provide critical information about a leak of incredibly sensitive data. Instead, he reported the clinic to the FTC, provided information on the leak to an attorney, and provided certain services to the attorney free of charge but not to the clinic at all.

Boback's actions on behalf of Tiversa demonstrate that when, in a position to prevent harm to companies or the federal government, he acted to benefit himself and Tiversa. Federal departments and agencies should be aware of these business practices when determining whether to do business with Tiversa.